TP-LINK®

User Guide

Archer CR700

AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router

Rev: 1.0.0
1910011153

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

http://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

CE 1588 ⓘ

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don’t use the product outdoors in France.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1)This device may not cause interference, and

(2)This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux norms CNR exemptes de licence d’Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes:

(1)cet appareil ne doit pas provoquer d’interférences et

(2)cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l’appareil.

Industry Canada Statement

Complies with the Canadian ICES-003 Class B specifications.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with RSS 210 of Industry Canada. This Class B device meets all the requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la Classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice& BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

●請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。

●清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。

●注意防潮，請勿將水或其他液體潑灑到本產品上。 □

●插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。

●請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。

●請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don’t disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.

- Avoid water and wet locations.

This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA	US		

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router

Model No.: **Archer CR700**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

The above product is in conformity with the following standards or other normative documents

EN 300 328 V1.8.1

EN 301 489-1 V1.9.2 & EN 301 489-17 V2.2.1

EN 55022: 2010 + AC: 2011

EN 55024: 2010

EN 61000-3-2: 2006 + A1: 2009 + A2: 2009

EN 61000-3-3: 2013

EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011

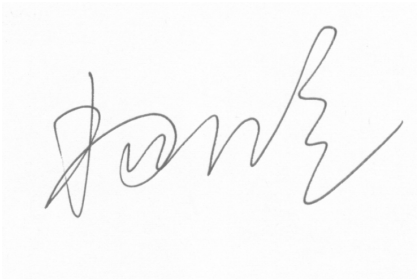
EN 50385: 2002

EN 301 893 V1.7.1

The product carries the CE Mark:

CE1588 ①

Person responsible for making this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue: 2014

TP-LINK TECHNOLOGIES CO., LTD

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park, Shennan Rd, Nanshan, Shenzhen, China

CONTENTS

Package Contents **1**

Chapter 1. Product Overview **2**

1.1 Overview of the Modem Router 2

1.2 Main Features 2

1.3 Panel Layout 4

1.3.1 The Front Panel 4

1.3.2 The Back Panel 6

Chapter 2. Connecting the Modem Router **7**

2.1 System Requirements 7

2.2 Installation Environment Requirements 7

2.3 Connecting the Modem Router 7

Chapter 3. Configure the Modem Router **10**

Chapter 4. Basic **12**

4.1 Network Map 12

4.2 Internet 12

4.3 Wireless 15

4.4 Guest Network 16

4.5 USB Settings 18

4.5.1 Folder Sharing 18

4.5.2 Print Server 21

4.6 Parental Control 21

Chapter 5. Advanced **25**

5.1 Status 25

5.2 Operation Mode 25

5.3 Network 26

5.3.1 WAN 26

5.3.2 LAN Settings 33

5.3.3 IPv6 LAN Settings 34

5.3.4 Dynamic DNS 36

5.3.5 Advanced Routing 37

5.4 Wireless 2.4G 38
5.4.1 Basic Settings 38
5.4.2 Primary Network 39
5.4.3 Guest Network 43
5.4.4 Wireless Advanced 45
5.4.5 MAC Filtering 46
5.4.6 Wireless Bridging 48
5.5 Wireless 5G 49
5.5.1 Basic Settings 49
5.5.2 Primary Network 50
5.5.3 Guest Network 54
5.5.4 MAC Filtering 56
5.5.5 Wireless Bridging 58
5.5.6 Wireless Advanced 59
5.6 NAT Forwarding 60
5.6.1 IP Filtering 60
5.6.2 MAC Filtering 61
5.6.3 Port Filtering 62
5.6.4 Port Forwarding 63
5.6.5 Port Triggers 65
5.6.6 DMZ 68
5.6.7 Options 68
5.7 USB Settings 69
5.7.1 Disk Settings 70
5.7.2 Folder Sharing 70
5.7.3 Print Server 73
5.8 Firewall 74
5.8.1 Basic 74
5.8.2 Local Log 74
5.8.3 Remote Log 75
5.9 System Tools 76
5.9.1 System Information 76
5.9.2 Device Information 77
5.9.3 Connection Status 77
5.9.4 Diagnostic 78
5.9.5 Time Zone 79

5.9.6 Backup & Restore 80
5.9.7 Administrator 81
5.9.8 Event Log 83

Appendix A: Specifications 84

Appendix B: Technical Support 88

Package Contents

The following contents should be found in your package:

- One Archer CR700 AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router
- One Power Adapter for Archer CR700 AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router
- Quick Installation Guide
- One RJ45 cable

Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1. Product Overview

Thank you for choosing the **Archer CR700 AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router**.

1.1 Overview of the Modem Router

The Archer CR700 AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router integrates DOCSIS 3.0 modem, NAT router, 4-port switch and wireless access point in one device provides a one-stop networking solution.

The modem router provides up to 450Mbps (2.4GHz) + 1300Mbps (5GHz) wireless connection with other wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11ac wireless modem router will give you the unexpected networking experience at speed much faster than 802.11n. It is also compatible with all IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n, products.

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128 WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the Archer CR700 AC1750 Wireless Dual Band Gigabit DOCSIS 3.0 Cable Modem Router provides complete data privacy.

The modem router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staffs. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Since the modem router is compatible with virtually all the major operating systems, it is very easy to manage. Detailed instructions are provided step by step in this user guide. Before installing the modem router, please look through this guide to know all the modem router's functions.

1.2 Main Features

- Supports 802.11ac - The next generation of Wi-Fi
- Dual band – for combined wireless speeds of up to 1.75Gbps at 2.4GHz and 5GHz band concurrently
- DOCSIS 3.0, Compatible with DOCSIS 2.0/1.1/1.0
- 16 Downstream Channel bonding, Up to 680Mbps Downstream for DOCSIS and 900Mbps
- 4 Upstream Channel bonding, Up to 120Mbps Upstream
- Full Band Capture windows - Utilize any channels in the downstream spectrum.
- Dual-core processor –for wonderful performance with Internet, Wi-Fi, Ethernet and USB devices
- 6 internal antennas provide maximum Omni-directional wireless coverage and reliability
- Full gigabit ports ensure ultra fast data transfer speeds
- Dual USB Ports - easily share printers, files or media with your friends or family locally or over the Internet
- Guest Network Access provides secure Wi-Fi access for guests sharing your home or office

network

- IPv6 supported, meeting the demands for the next generation of Internet
- Wi-Fi On/Off Button allows users to turn their wireless radio on or off
- Easy one-touch WPA wireless security encryption with the WPS button
- WPA-PSK/WPA2-PSK encryptions provide user networks with active defense against security threats
- Parental Controls allow parents or administrators to establish restricted access policies for children or staff

1.3 Panel Layout

1.3.1 The Front Panel

Figure 1-1

The modem router's LEDs are located on the side panel (View from top to bottom). They indicate the device's working status. For details, please refer to LED Explanation.

LED Explanation:

Name	Status	Indication
⏻	On	The modem router is powered on.

(Power)	Off	The modem router is off. Please ensure that the power adapter is connected correctly.
(Downstream)	Orange	The modem router is synchronized to multiple downstream channels.
	White	The modem router is synchronized to a single downstream channel.
	Flash	Scanning for a downstream channel connection.
	Off	Failed to search non-bounded downstream channel.
(Upstream)	Orange	The modem router is synchronized to multiple upstream channels.
	White	The modem router is synchronized to a single upstream channel.
	Flash	Scanning for an upstream channel connection.
	Off	Failed to search non-bounded upstream channel.
(Online)	On	The network is available with a successful Internet connection.
	Off	There is no successful Internet connection.
(LAN)	On	There is a device connected to this LAN port.
	Off	There is no device connected to this LAN port.
(Wireless)	On	Wireless is enabled. The modem router is working on 2.4GHz/5 GHz radio band.
	Off	Wireless is disabled.
(WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Flash	WPS handshaking is in process and will continue for about 2 minutes. Please press the WPS button on other wireless devices that you want to add to the network while the LED is flashing.
	Off	A wireless device has failed to be added to the network by WPS function.
(USB on the back panel)	Off	No storage device or printer is plugged into the USB port.
	On	A storage device or printer has connected to the USB port.

1.3.2 The Back Panel

Figure 1-2

- **RESET**: There are two ways to reset the modem router's factory defaults.

  Method one: With the modem router powered on, use a pin to press and hold the Reset button for at least 8-10 seconds. And the modem router will reboot to its factory default settings.

  Method two: Restore the default setting from "5.9.6 Backup & Restore" of the modem router's Web-based Management.

- **WPS**: The switch for the WPS function.
- **WiFi ON/OFF**: The switch for the WiFi function. Press it to enable/disable the WiFi function.
- **USB2, USB1**: The USB port connects to a USB storage device or a USB printer.
- **LAN4, LAN3, LAN2, LAN1:** Through these ports, you can connect the modem router to your PC or the other Ethernet network devices.
- **Cable:**
- **DC**: The power plug where you will connect the power adapter.
- **Power ON/OFF**: The switch for the power.

Chapter 2. Connecting the Modem Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet).
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

2.2 Installation Environment Requirements

- The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- The Router can be placed on a shelf or desktop.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

2.3 Connecting the Modem Router

Before installing the device, please make sure your broadband cable service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.

Step 1: Connect the coaxial cable to the modem router.

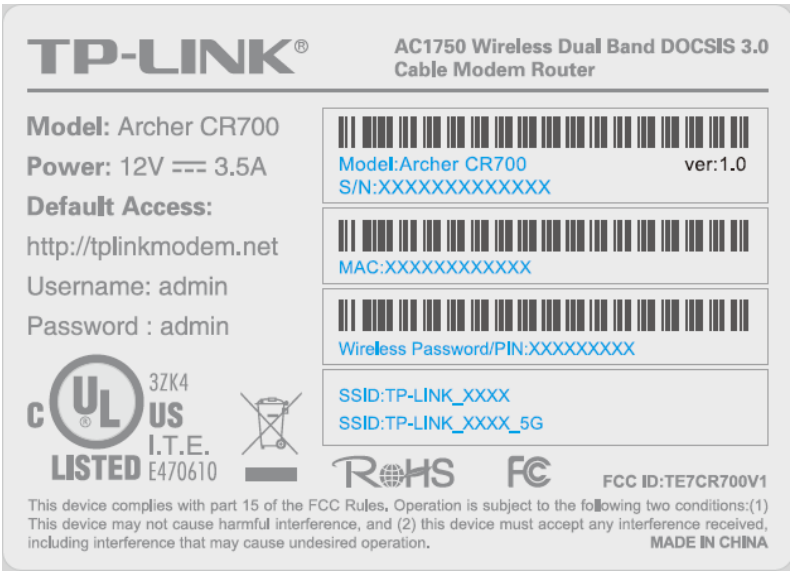
Step 2: Power on your modem router.

Step 3: Connect your computer to the router with an Ethernet cable or wirelessly. You can connect wirelessly by using the default SSID (Wireless Network Name) and password printed on the product label at the bottom of the Archer CR700.

Step 4: Wait for two minutes. Make sure the following LEDs are on as indicated below.

- **Power**: Solid
- **Downstream**: Solid
- **Upstream**: Solid
- **Online**: Solid or Flashing
- **Wireless**: Solid

Step 5: Contact your Internet Service Provider (ISP) to activate the Archer CR700 with the information below.



Step 6: Open a web browser and type in a valid URL, for example, http://www.tp-link.com, to test the Internet connection.

Note:

If the Internet is not accessible, please contact your ISP to make sure that the modem router is activated successfully.

For advanced configuration, go to the web management page at http://tplinkmodem.net or 192.168.1.1, and use admin (all lowercase) for both user name and password to log in.

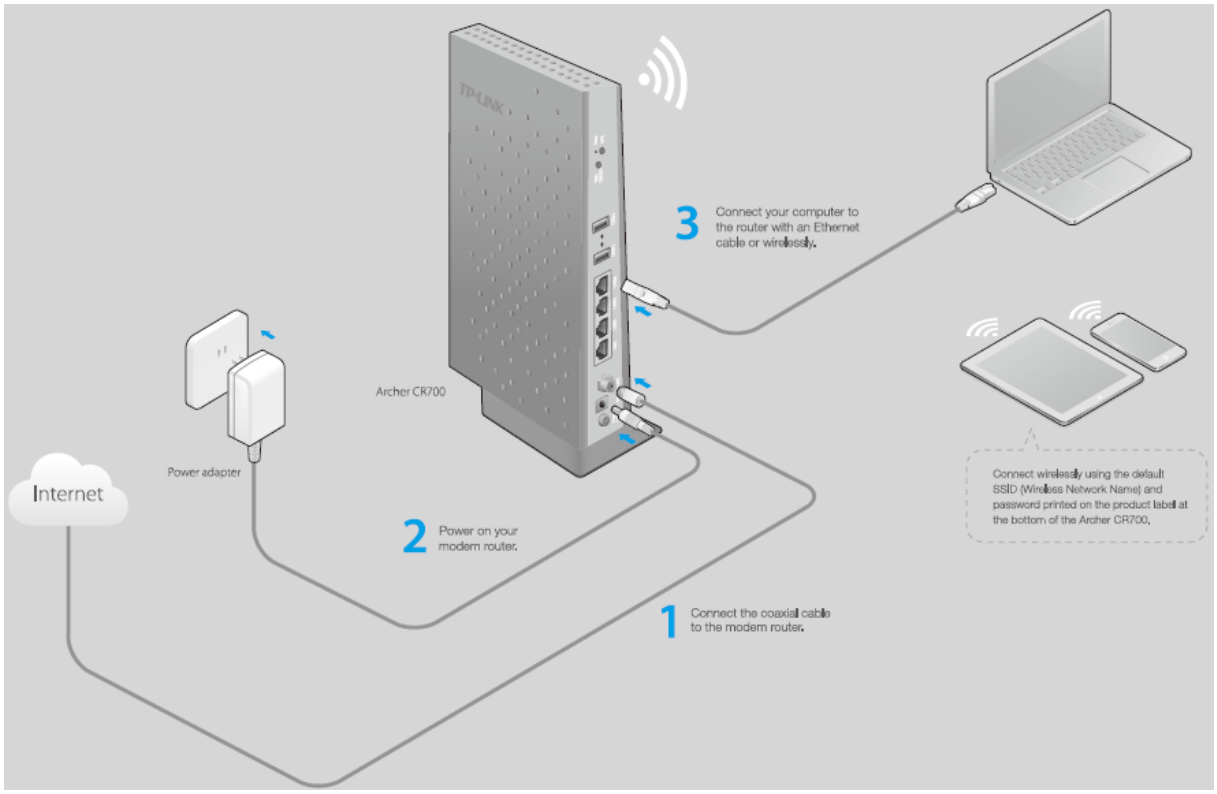


Figure 2-1

The cable distribution system should be grounded (earthed) in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of Outer Conductive Shield of a Coaxial Cable.

Chapter 3. Configure the Modem Router

With a Web-based management page, it is easy to configure and manage the Archer CR700 AC1750 Wireless Dual Band DOCSIS 3.0 Cable Modem Router. The Web-based management page can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

To access the configuration utility, open a web-browser and type the default address http://tplinkmodem.net/ or 192.168.1.1 in the address field of the browser.

Figure 3-1

After a moment, a login window will appear, similar to the Figure 3-2. Enter **admin** for the Username and Password, both in lower case letters. Then click the **Login** button or press the Enter key.

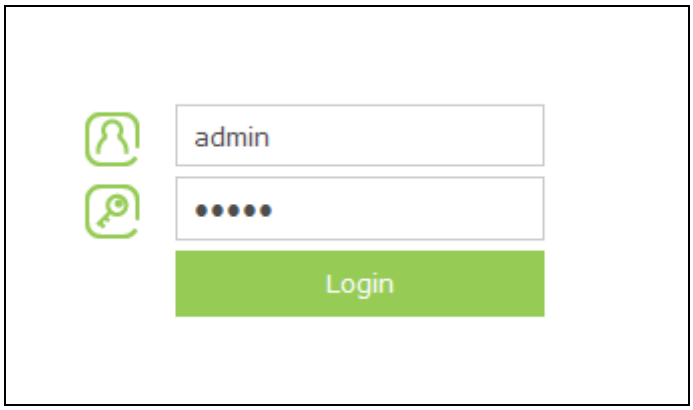


Figure 3-2

After your successful login, you will see the screen as shown in Figure 3-3.

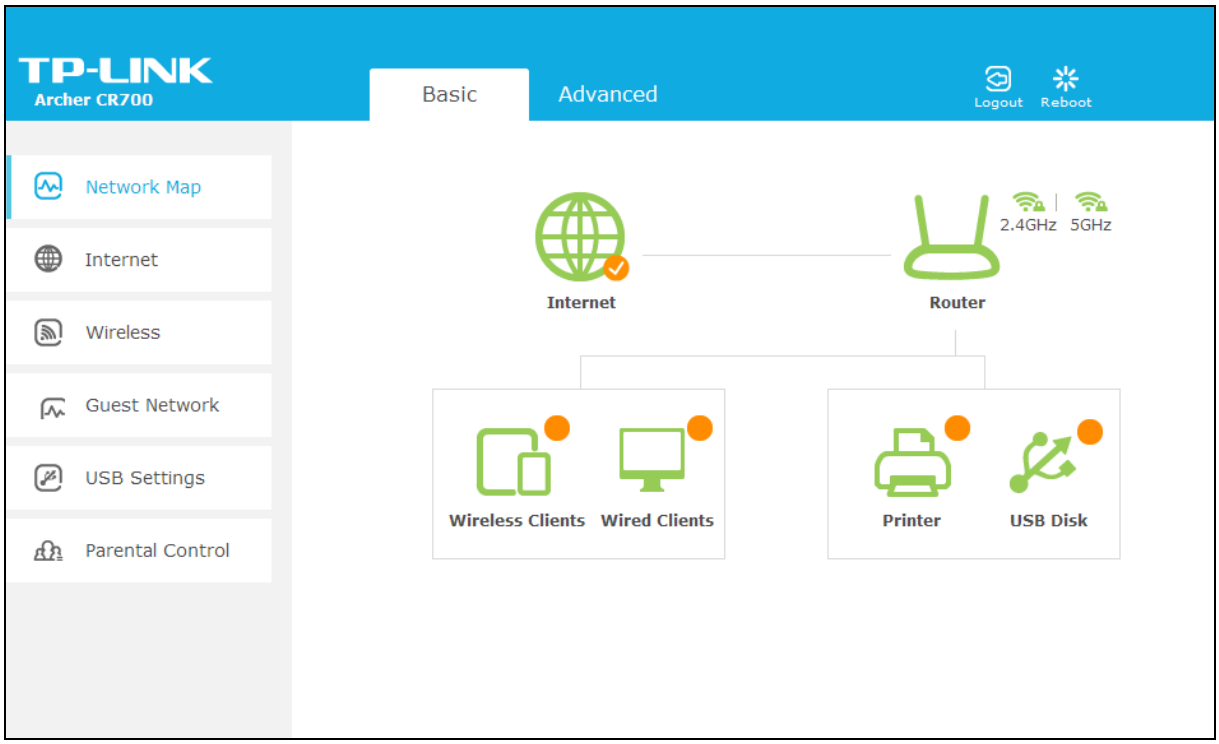


Figure 3-3

The detailed explanations for each Web page's key function are listed below.

Chapter 4. Basic

4.1 Network Map

Network Map provides a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the eight sections of the dashboard to view the detail information. All the information is read-only.

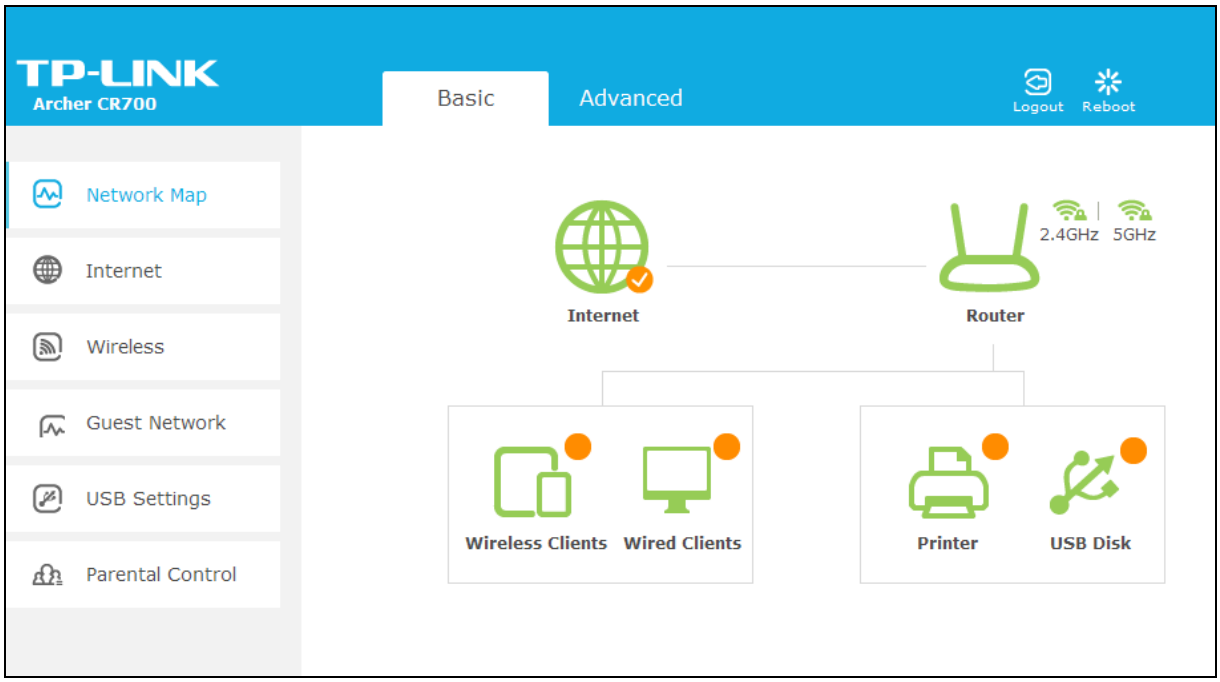


Figure 4-1

- **Internet -** View Check the ISP settings of your modem router.
- **Router -** View Check the Wireless and Guest Network settings.
- **Wireless Clients -** Click to view the wireless devices connected to your network.
- **Wired Clients -** Click to view the wired devices connected to your network.
- **Printer -** Click to view the information of the printer connected to your network.
- **USB Disk -** Click to view the information of the USB storage device connected to your network.

4.2 Internet

Choose "**Basic → Internet**", and you can configure the basic settings of the ISP Configuration and the Internet on this page.

There are four different connection types, Dynamic IP, Static IP, L2TP(Dynamic IP) and L2TP(Static). You can select the corresponding type according to your needs.

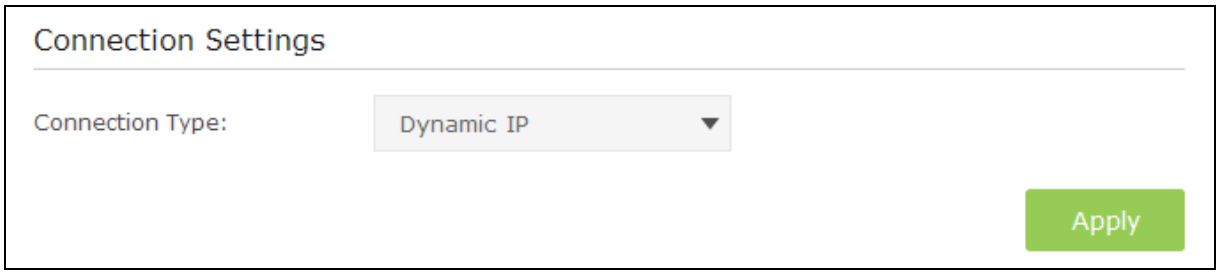


Figure 4-2

1) Dynamic IP

Choose **Dynamic IP** in the drop-down list, the modem router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP.

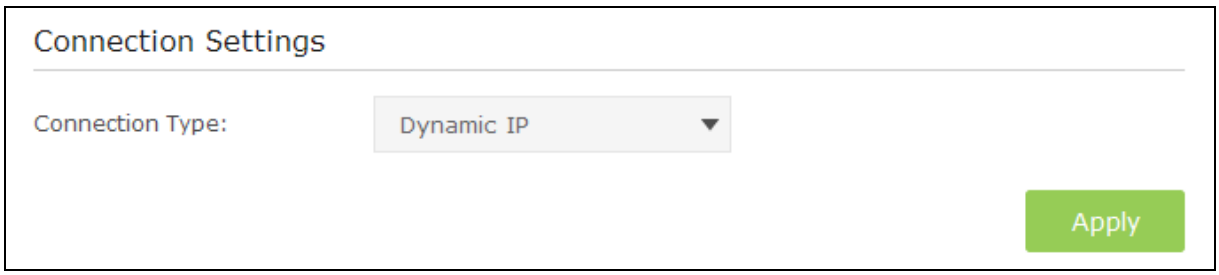


Figure 4-3

Click the **Apply** button to save the settings.

2) Static IP

Choose **Static IP** in the drop-down list if your ISP provides static IP information to you. You should set static IP address, Subnet mask, and gateway address in the screen below.

Figure 4-4

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.

- **Primary DNS/ Secondary DNS -** Here you can set DNS Server (at least one) manually. The Route will use this DNS Server for priority.

Click the **Apply** button to save the settings.

3) L2TP(Dynamic IP)

Choose **L2TP(Dynamic IP)** in the drop-down list if your ISP provides L2TP(Dynamic IP) information to you. You should set User name, Password and Server IP Address/Name in the screen below.

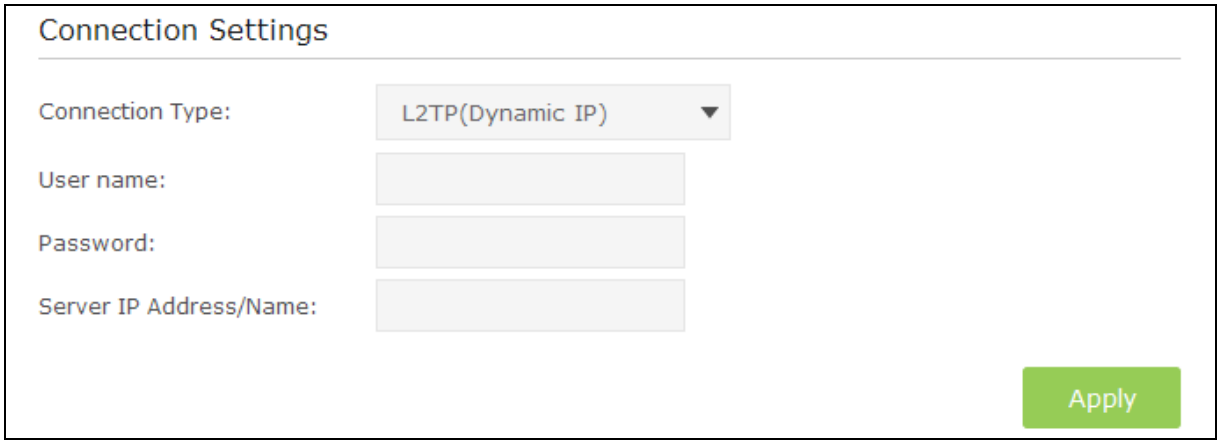


Figure 4-5

- **Username/Password -** Enter the **Username** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.
- **Server IP Address/Name -** Enter the server IP address or domain name provided by your ISP. If you have difficulty with this process, please contact your ISP.

Click the **Apply** button to save the settings.

4) L2TP(Static)

Choose **L2TP(Static)** in the drop-down list if your ISP provides L2TP(Static) information to you. You should set User name, Password, Server IP Address/Name, IP Address, Subnet Mask and Default Gateway in the screen below.

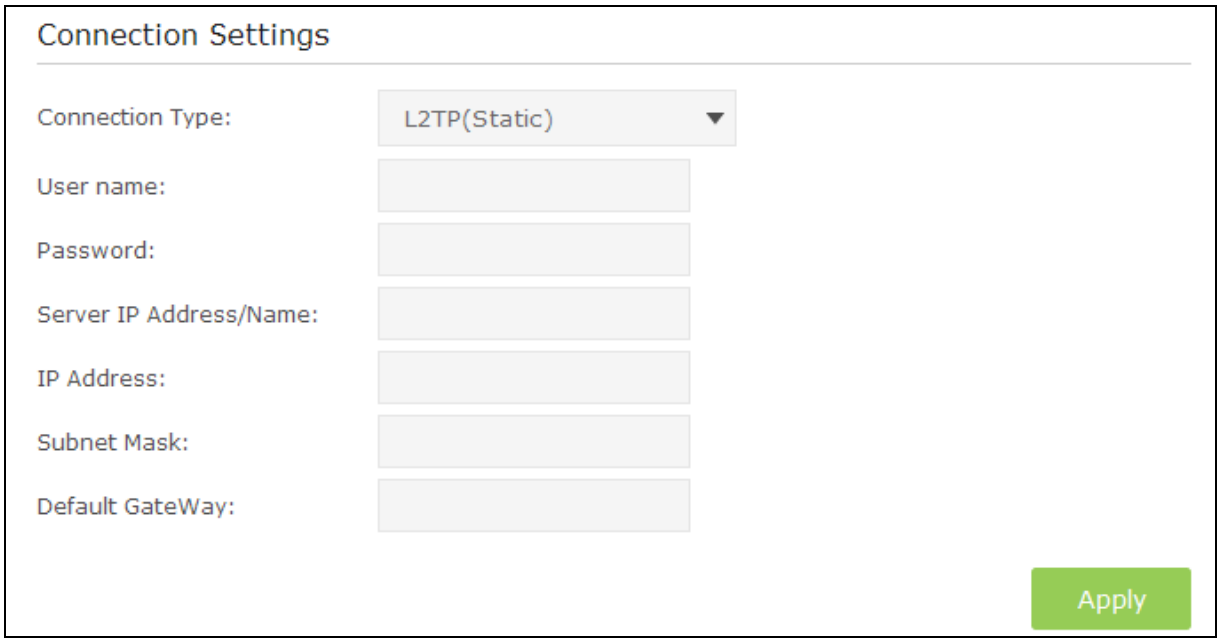


Figure 4-6

- **Username/Password -** Enter the **Username** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.
- **Server IP Address/Name -** Enter the server IP address or domain name provided by your ISP. If you have difficulty with this process, please contact your ISP.
- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.

Click the **Apply** button to save the settings.

4.3 Wireless

Choose menu "**Basic**" → "**Wireless**", you can configure the basic settings for the wireless networks of 2.4GHz and 5GHz on this page.

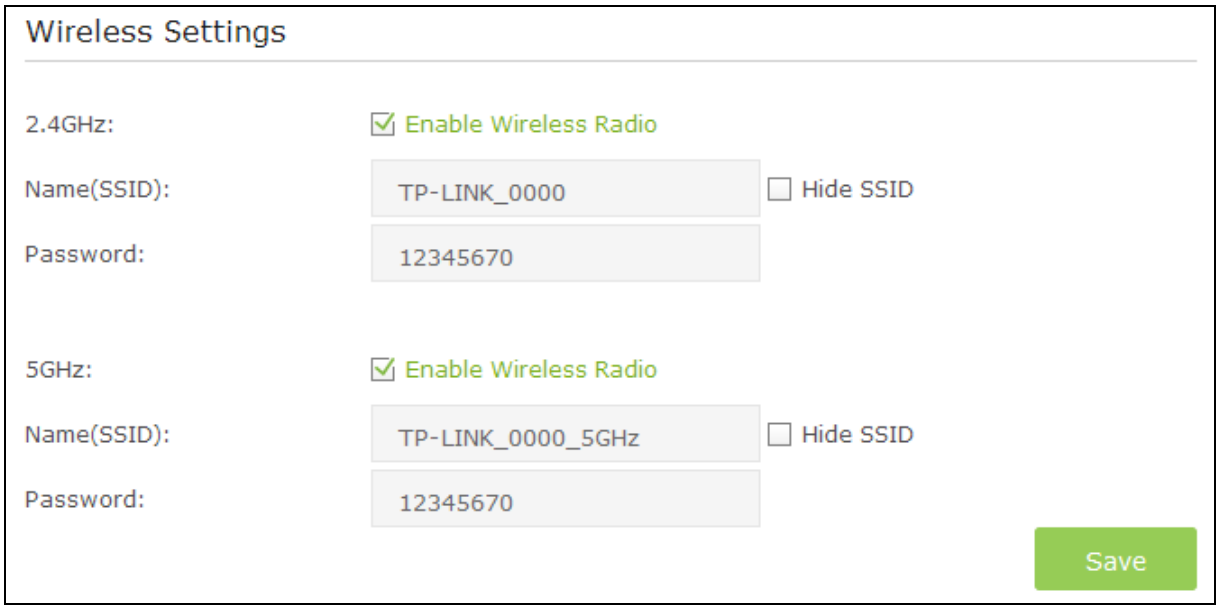


Figure 4-7

- **Enable Wireless Radio –** Check the box to enable the Wireless Radio.
- **Name (SSID) –** Create a name (up to 32 characters) for your 2.4GHz/5GHz wireless network. The default SSID is set to be TP-LINK_XXXX for the wireless network of 2.4GHz and TP-LINK_XXXX _5G for the wireless network of 5GHz.
- **Hide SSID –** If you want to hide the SSID of your wireless network from the Wi-Fi network, you should check the box.
- **Password –**You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the back of the modem router.

Click the **Save** button to save the settings.

4.4 Guest Network

Choose menu "**Basic → Guest Network**", and you will see the screen as shown in Figure 4-8. This feature allows you to create a separate network for your guests without allowing them to access your main network and the computers connected to it.

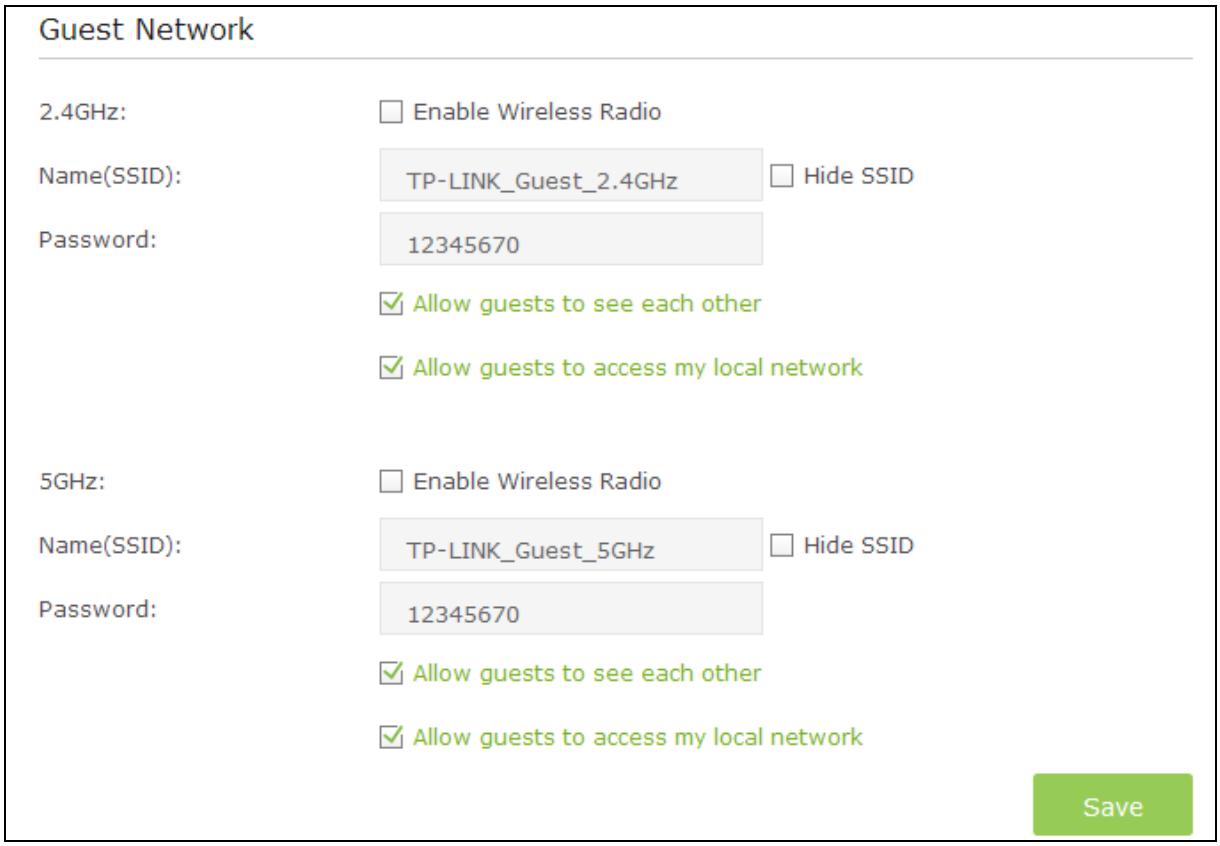


Figure 4-8

- **2.4GHz -** If **Enable Wireless Radio** is selected, please complete the following parameters.

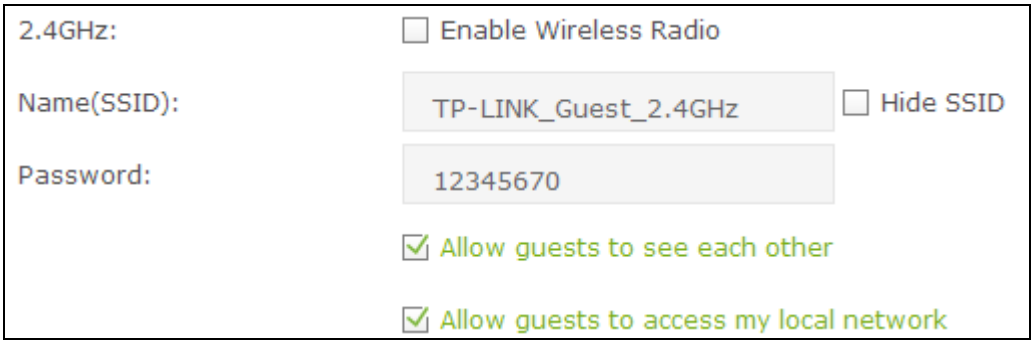


Figure 4-9

- **Name (SSID) -** Create a name for the guest network. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network. The default name is TP-LINK_Guest_2.4GHz. If you want to hide the guest network from the Wi-Fi network, check the **Hide SSID**.
- **Password -** Create a password for the guest network. The password must have a minimum of 8 characters in length.
- **Allow guests to see each other -** If **Allow guests to see each other** is selected, anyone who connects to the guest network can **access** each other.
- **Allow guests to access my local network -** If **Allow guests to access my local network** is selected, anyone who connects to the guest network has access to your local network, not just Internet access.

- **5GHz -** If **Enable Wireless Radio** is selected, please complete the following parameters.

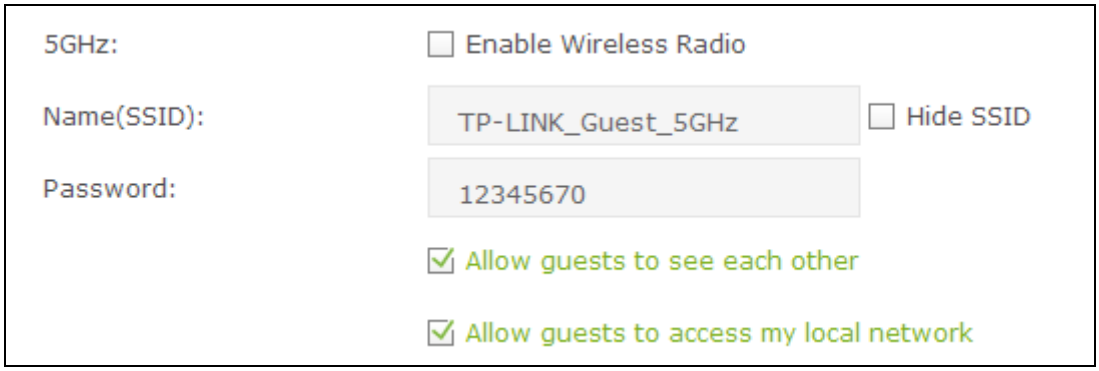


Figure 4-10

- **Network Name(SSID) -** Create a name for the guest network. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network. The default name is TP-LINK_Guest_XXXX_5G. If you want to hide the guest network from the Wi-Fi network, check the **Hide SSID**.
- **Security -** It's strongly recommended to select **Set a password**. If you do not want to use wireless security, choose **None**.
- **Password -** Create a password for the guest network. The password must have a minimum of 8 characters in length.
- **Allow guests to see each other -** If **Allow guests to see each other** is selected, anyone who connects to the guest network can **access** each other.
- **Allow guests to access my local network -** If **Allow guests to access my local network** is selected, anyone who connects to the guest network has access to your local network, not just Internet access.

Click the **Save** button to save the settings.

4.5 USB Settings

There are three submenus under the USB Settings menu, **Folder Sharing** and **Print Server.** Click any of them, and you will be able to configure the corresponding function.

4.5.1 Folder Sharing

Choose menu "**Basic → USB Settings → Folder Sharing**", you can view the basic information about the connected USB mass storage, and configure Sharing Folders(Media file, Document files, Compress files and so on.)

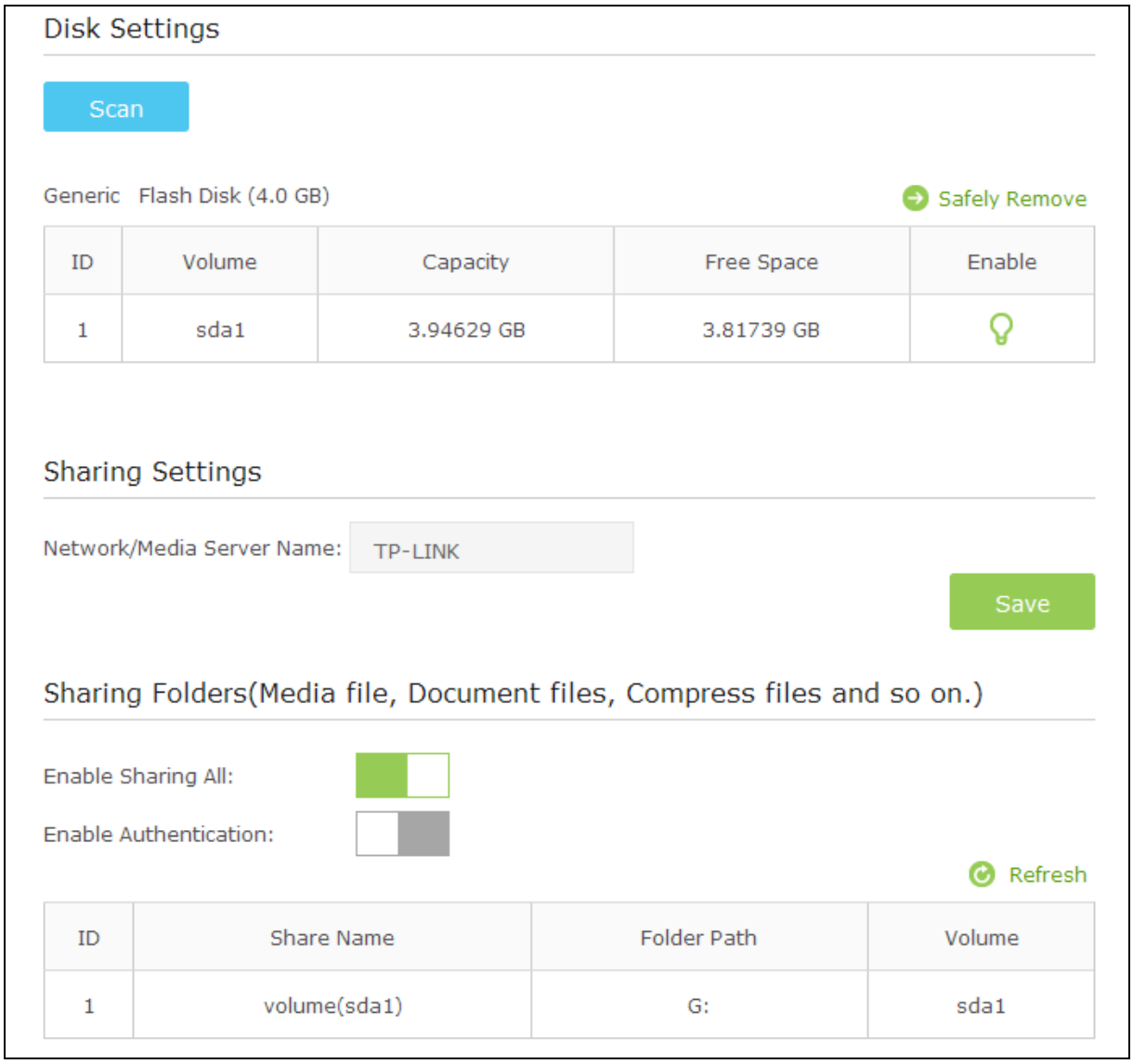


Figure 4-11 Folder Sharing

Disk Settings:

- **Scan -** Click the button to display the information of the USB storage device connected to the modem router.
- **Volume -** The volume name of the USB drive the users have access to.
- **Capacity -** The storage capacity of the USB driver.
- **Free Space -** The available capacity of the USB driver.
- **Enable -** When the volume is shared, you can click the icon to stop sharing the volume; when volume is non-shared, you can click the icon to share the volume.

Click **Safely Remove** button to remove the USB storage device that is connected to USB port.

Note:

Before removing the USB storage device, you should click "Safely Remove" to make sure that all your data have been saved completely. Removing device directly may cause your USB storage device crashed.

Sharing Settings:

- **Network/Media Server Name -** Show the name of the network/media server. This is the name used to access the USB device connected to the modem router.

Sharing Folders(Media file, Document files, Compress files and so on.):

- **Enable Sharing All -** The switch for sharing all the folders. If turn on the switch, the field will become green and all the folders in the USB drive will be shared.
- **Enable Authentication -** If turn on this switch, the folder sharing is need authentication. The default setting is off.

To share the folders you specified, please follow the steps below.

1. Turn off the **Enable Sharing All** switch and the next screen will pop-up as shown in Figure 4-12.

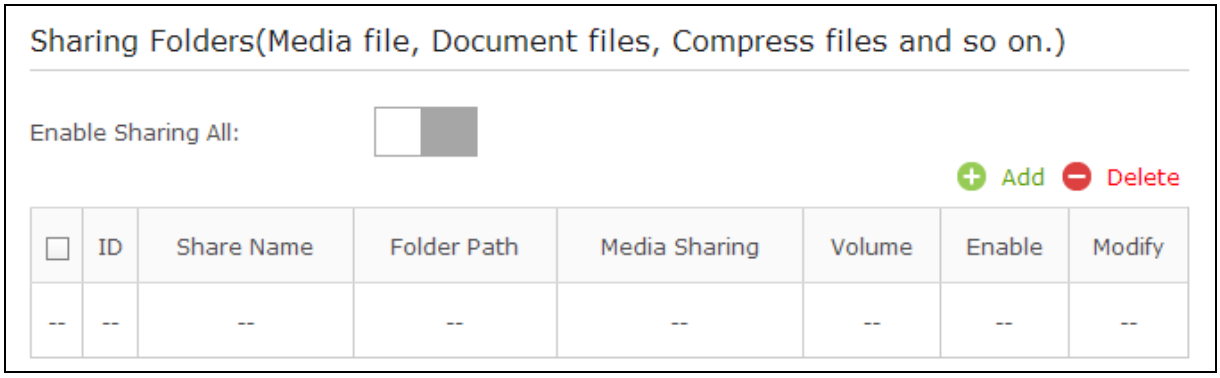


Figure 4-12 Add or Modify Share Folder

2. Click the **Add** button and the next screen will pop-up as shown in Figure 4-13.

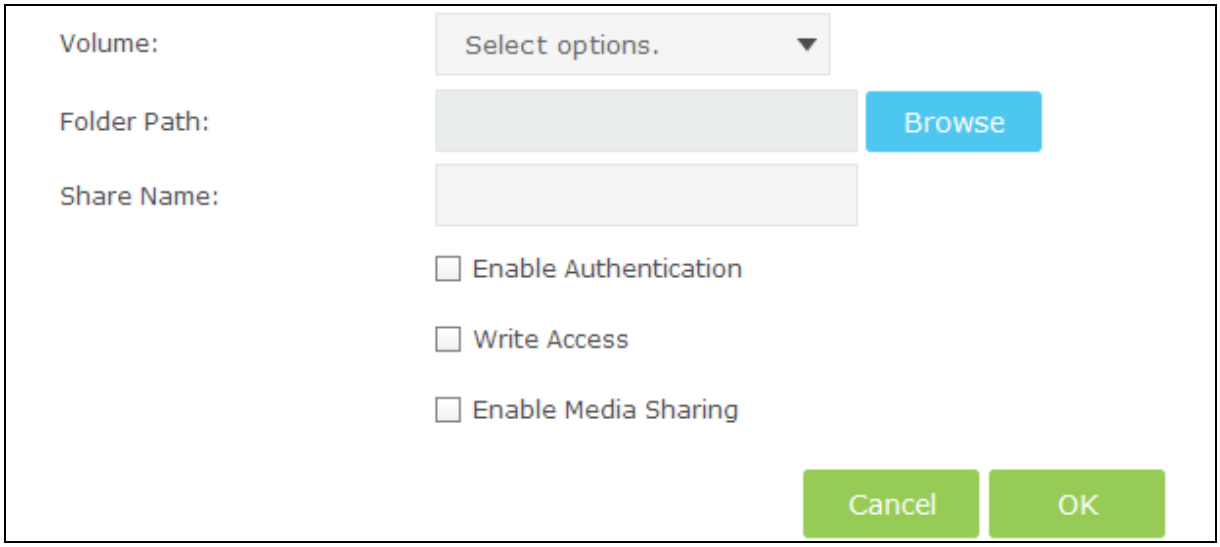


Figure 4-13 Add Share Folder

3. Select the volume desired to share from the **Volume** drop-down list. Then click the **Browse** button to select the folder path. You can create a share name, e.g. music.

4. Select the checkboxes in Figure 4-13.according to your needs.
   - **Enable Authentication -** If this checkbox is selected, then the folder sharing is need authentication.
   - **Write Access -** If this checkbox is selected, then the sharing folder is allowed write access.
   - **Enable Media Sharing -** Select this checkbox to enable media sharing.

Click **OK** to complete the settings.

4.5.2 Print Server

Choose menu "**Basic→USB Settings→Print Server**", you can enable or disable the print server.

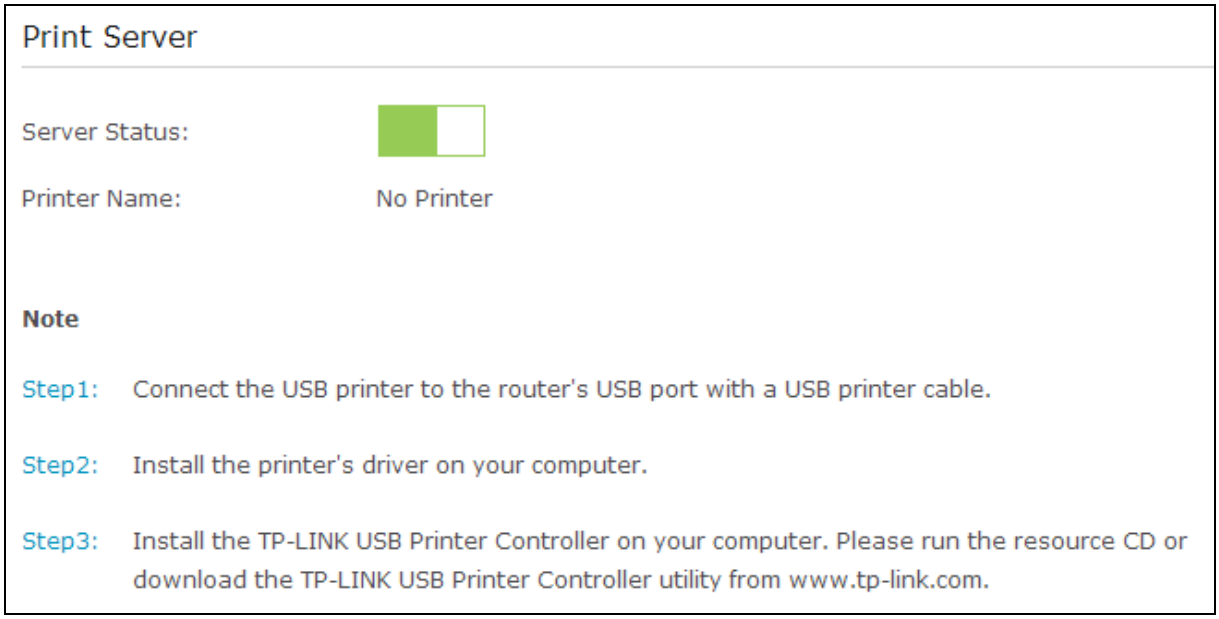


Figure 4-14 Print Server

4.6 Parental Control

Choose menu "**Basic→Parental Control**", and then you can configure the parental control. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

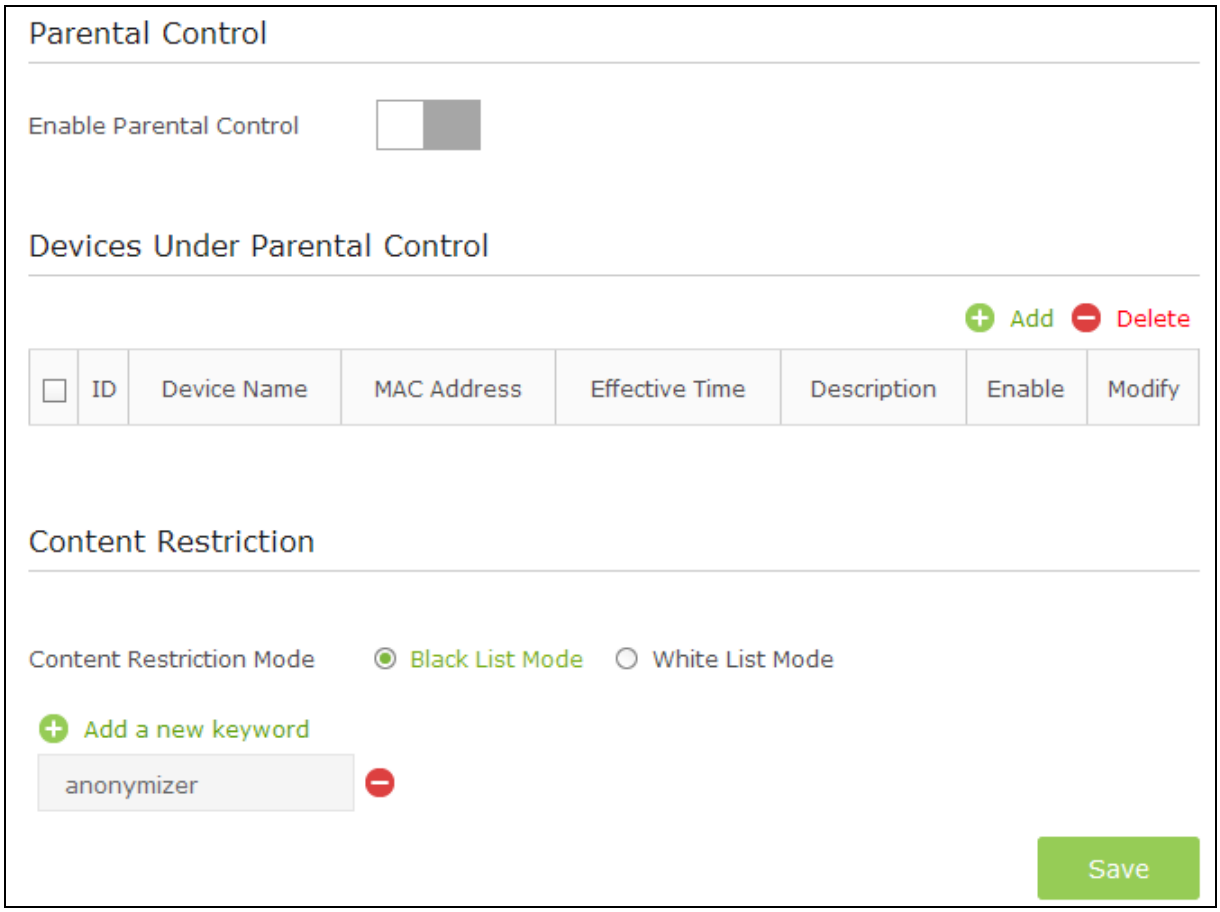


Figure 4-15 Parental Control Settings

Parental Control:

- **Enable Parental Control -** The switch for the parental control. If turn on the switch, the field will become green

Devices Under Parental Control:

- **Add -** You can add a new device for the parental control by clicking this button.
- **Delete -** You can click the button to delete the selected entries.
- **Device Name -**The name used for identifying a device.
- **MAC Address -** This field displays the MAC address of the PC that is managing this modem router.
- **Effective Time -** The time period allowed for the PC controlled to access the Internet. You can click the icon to configure the time period.
- **Description -** Here displays the description about the parental control and this description is unique.
- **Enable –** Click the icon to enable the function. If this function has taken effect, the icon will become .
- **Modify –** Click the icon to edit the corresponding entry. If you want to delete this entry, you can click the icon.

To add a new entry, please follow the steps below.

1. Click the **Add** button and the next screen will pop-up.

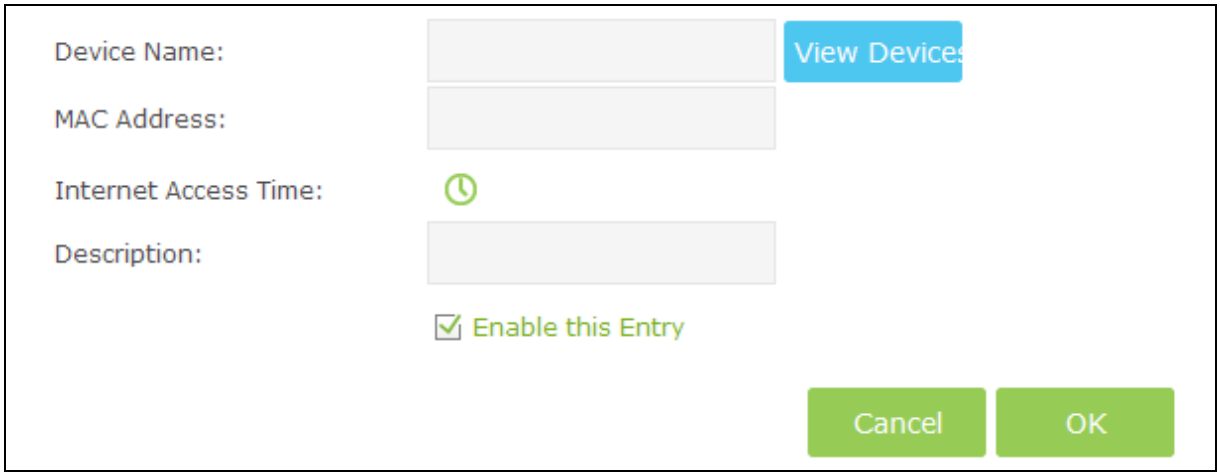


Figure 4-16 Add Parental Control Entry

2. Click **View Device** button and the next screen will pop-up. You'd like to click the icon to select a device.

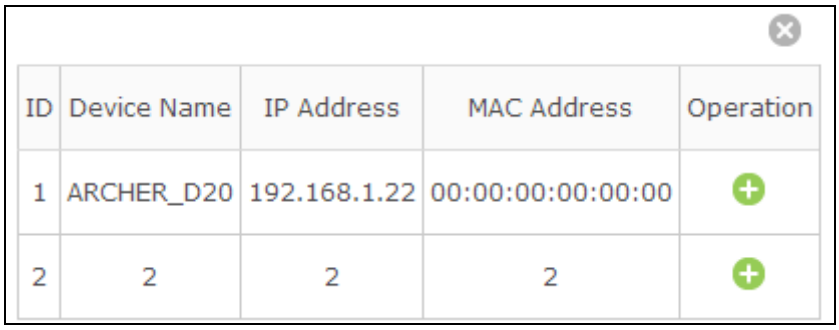
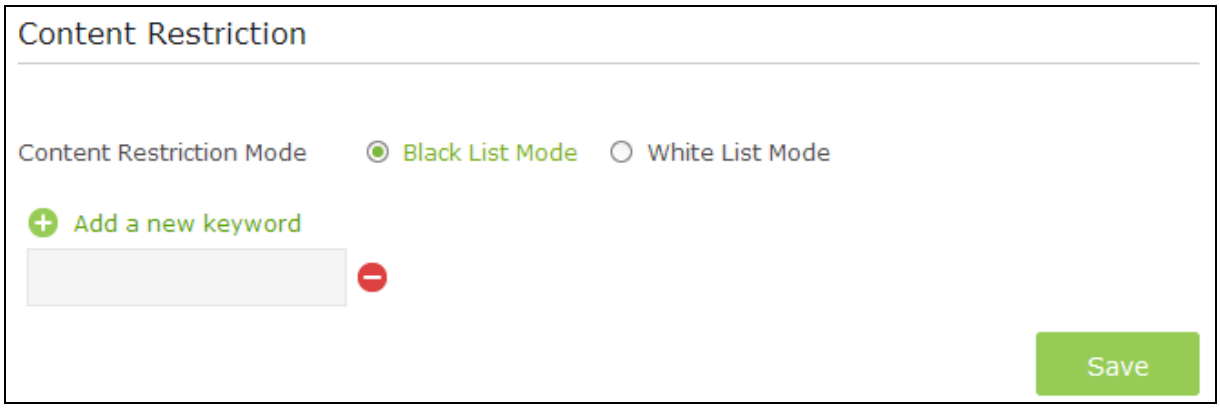


Figure 4-17 select a device

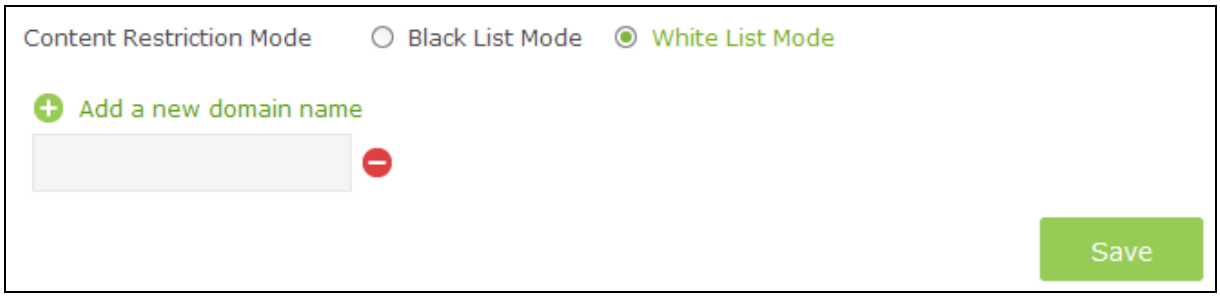
3. Click to create a new schedule. You'd like to click the Schedule in green below to go to the Advance Schedule Settings page and create the schedule you need. Then enter the **Description**.
4. Check the box **Enable this Entry** to enable this function.
5. Click **OK** to complete the settings.

Content Restriction:

- **Content Restriction Mode –** Select the **Black List Mode** or **White List Mode** for this account.
- **Black List Mode -** All webs entered within the Black List will be denied to access. Check the box to enable this mode. You'd like to click **Add a new keyword** button and input the net addresses which the child is denied to access.



- **White List Mode -** Only the web entered within the White List will be allowed. Check the box to enable this mode. You'd like to click **Add a new keyword** button and input the net addresses which the child is allowed to access.



Click **Save** to complete the settings.

Chapter 5. Advanced

5.1 Status

Choose menu "**Advanced→Status**", you can see the current status information about the modem router.

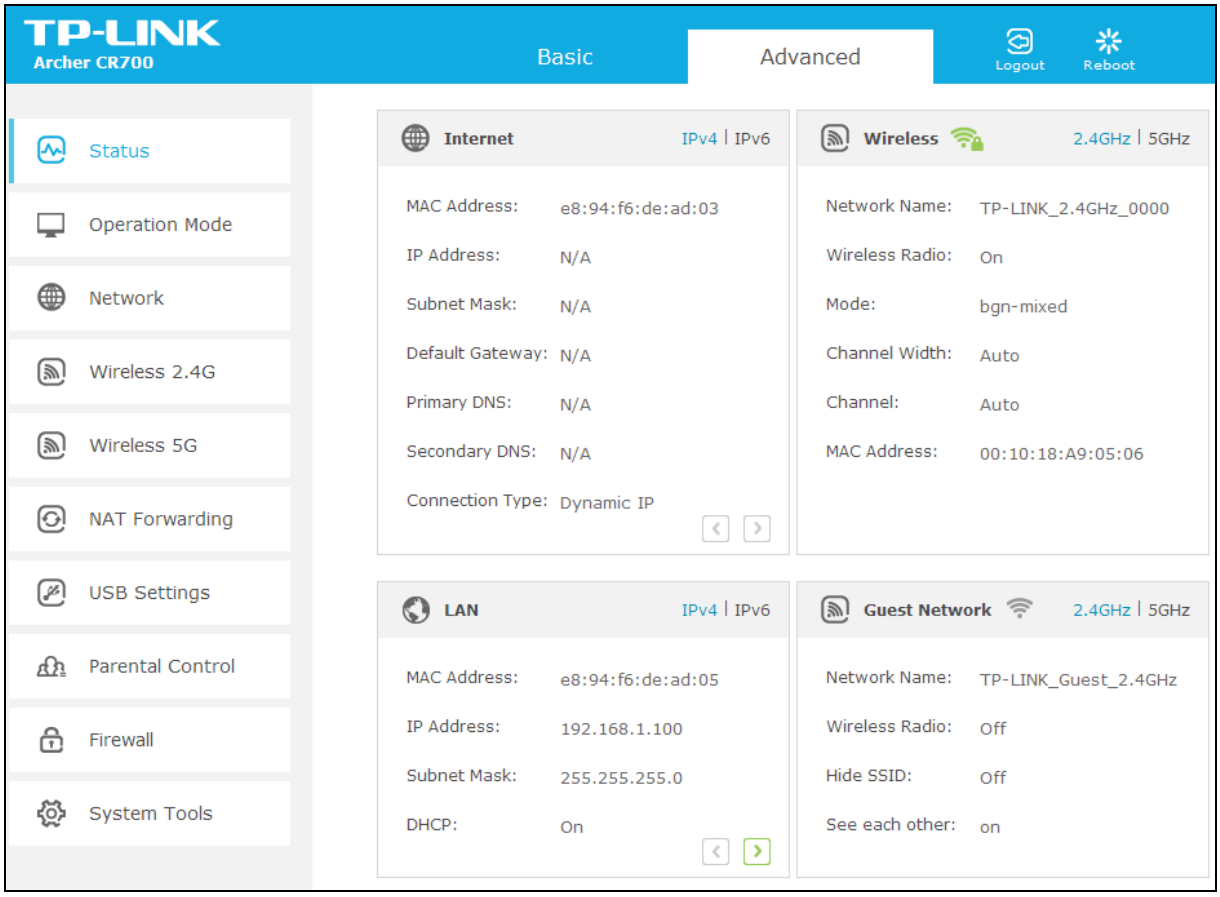


Figure 5-1 Status

5.2 Operation Mode

Choose menu "**Advanced→Operation Mode**", and you will see the screen as shown in Figure 5-2.Select your desired mode and then click **Save**.

Figure 5-2 Operation Mode

- **Router Mode -** The device enables multi-users to share Internet via Ethernet WAN (EWAN) using its interchangeable LAN4/WAN port and share it wirelessly at 450Mbps wireless speeds over the crystal clear 5GHz band and 1300Mbps over the 2.4GHz band.
- **Bridge Mode –** In this mode, the modem router can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

After you click the **Save** button, the modem router will reboot. Please wait.

5.3 Network

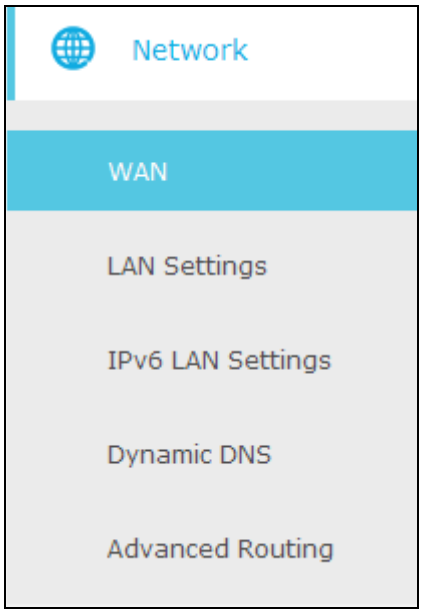


Figure 5-3 the Network menu

There are five submenus under the Network menu as shown in Figure 5-3: **WAN, LAN Settings**, **IPv6 LAN Settings**, **Dynamic DNS** and **Advanced Routing**. Click any of them, and you will be able to configure the corresponding function.

5.3.1 WAN

Choose "**Advanced →Network → WAN**", you can configure the IP parameters of the WAN on the screen below.

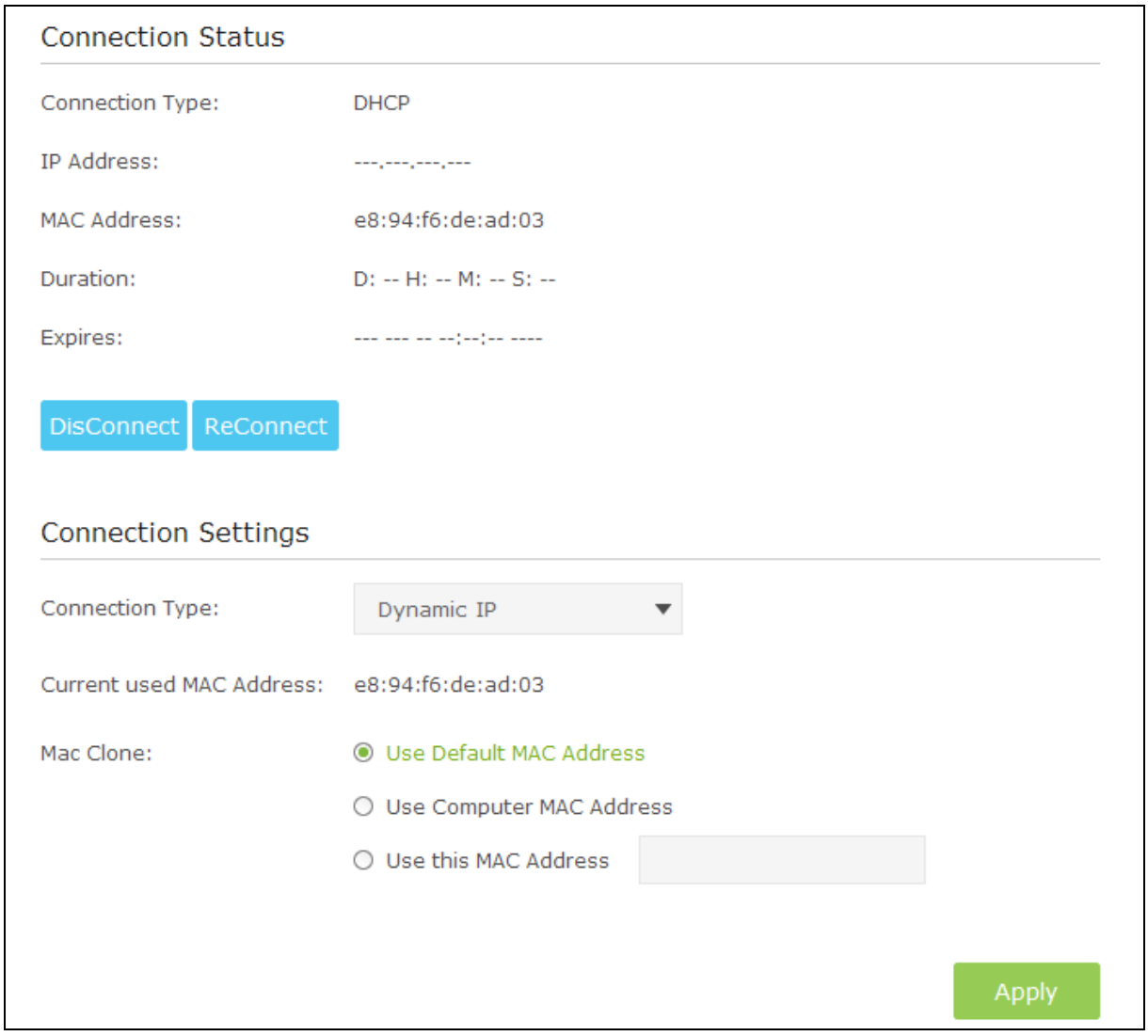
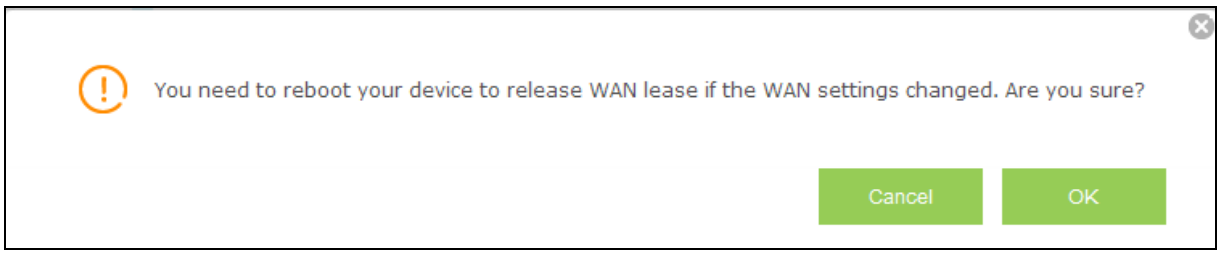


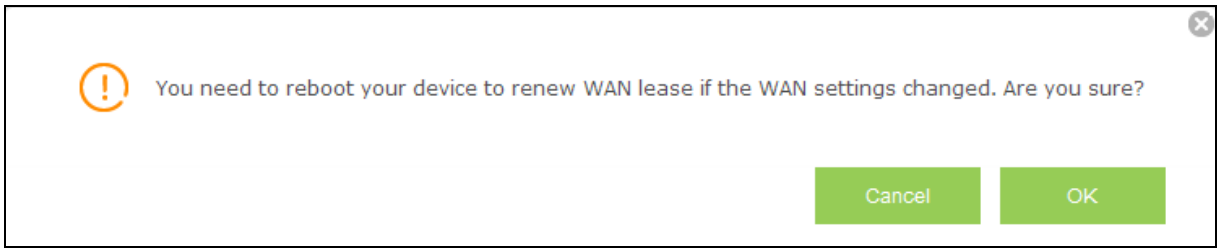
Figure 5-4

Connection Status:

- **Connection Type –** Display the connection type for WAN.
- **IP/MAC Address -** This field displays the current IP/MAC address of the Internet port.
- **Duration –** Display the total connection time.
- **Expires –** Display the expiration time of the DHCP servers leases an IP address to a new device.
- **DisConnect -** Click the **DisConnect** button to release WAN lease, then the Note Dialog will appear. You can click the **OK** button to disconnect immediately.



- **ReConnect –**Click the **ReConnect** button to renew WAN lease, then the Note Dialog will appear. You can click the **OK** button to disconnect immediately.



Connection settings:

There are four different connection types, Dynamic IP, Static IP, L2TP(Dynamic IP) and L2TP(Static). You can select the corresponding type according to your needs.

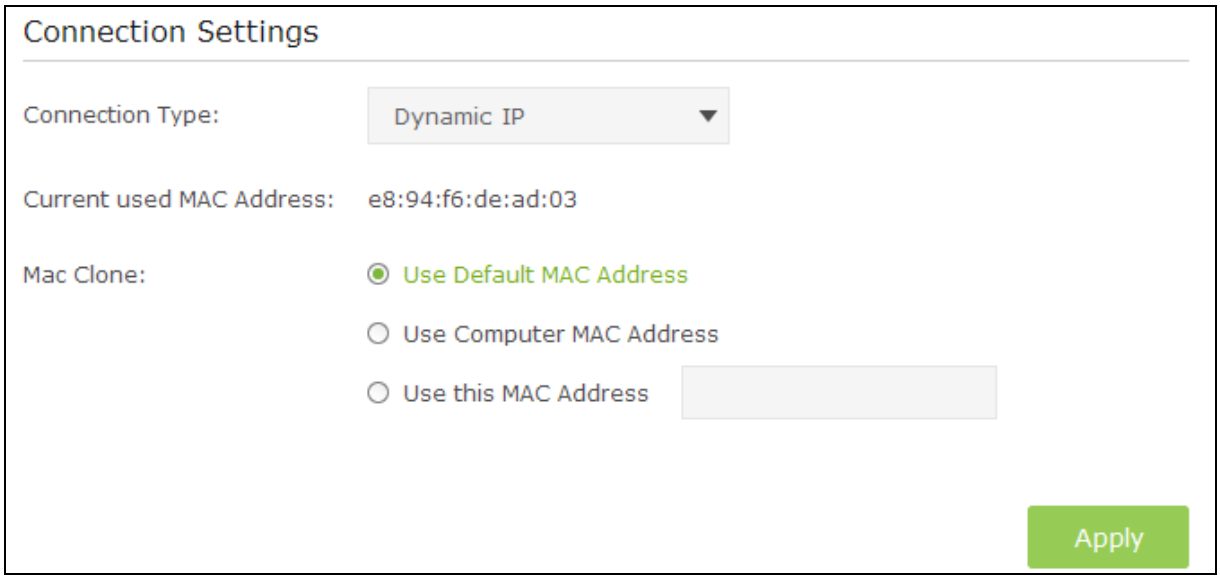


Figure 5-5 Connection settings

1) Dynamic IP

Choose **Dynamic IP** in the drop-down list, the modem router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP.

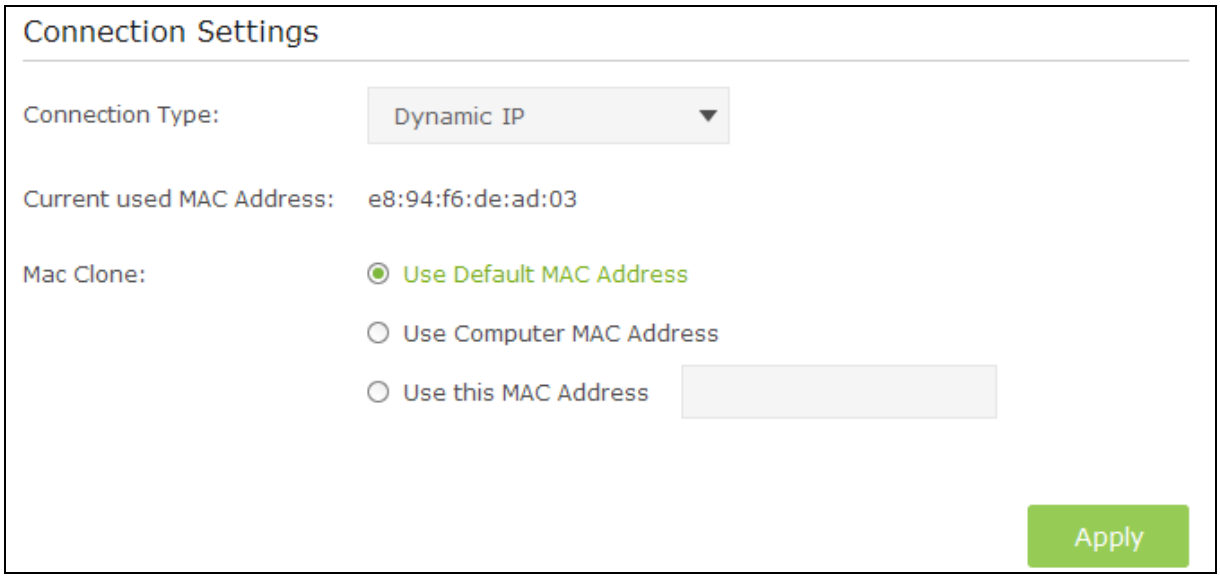


Figure 5-6 WAN - Dynamic IP

- **Current used MAC Address -** This field displays the current MAC address of the Internet port.
- **MAC Clone -** You can select one of below methods to change MAC address for this WAN Interface depend on your needs. If you select **Use this MAC Address**, you can enter the MAC Address you want to change.

Click the **Apply** button to save the settings.

2) Static IP

Choose **Static IP** in the drop-down list if your ISP provides static IP information to you. You should set static IP address, Subnet mask, and gateway address in the screen below.

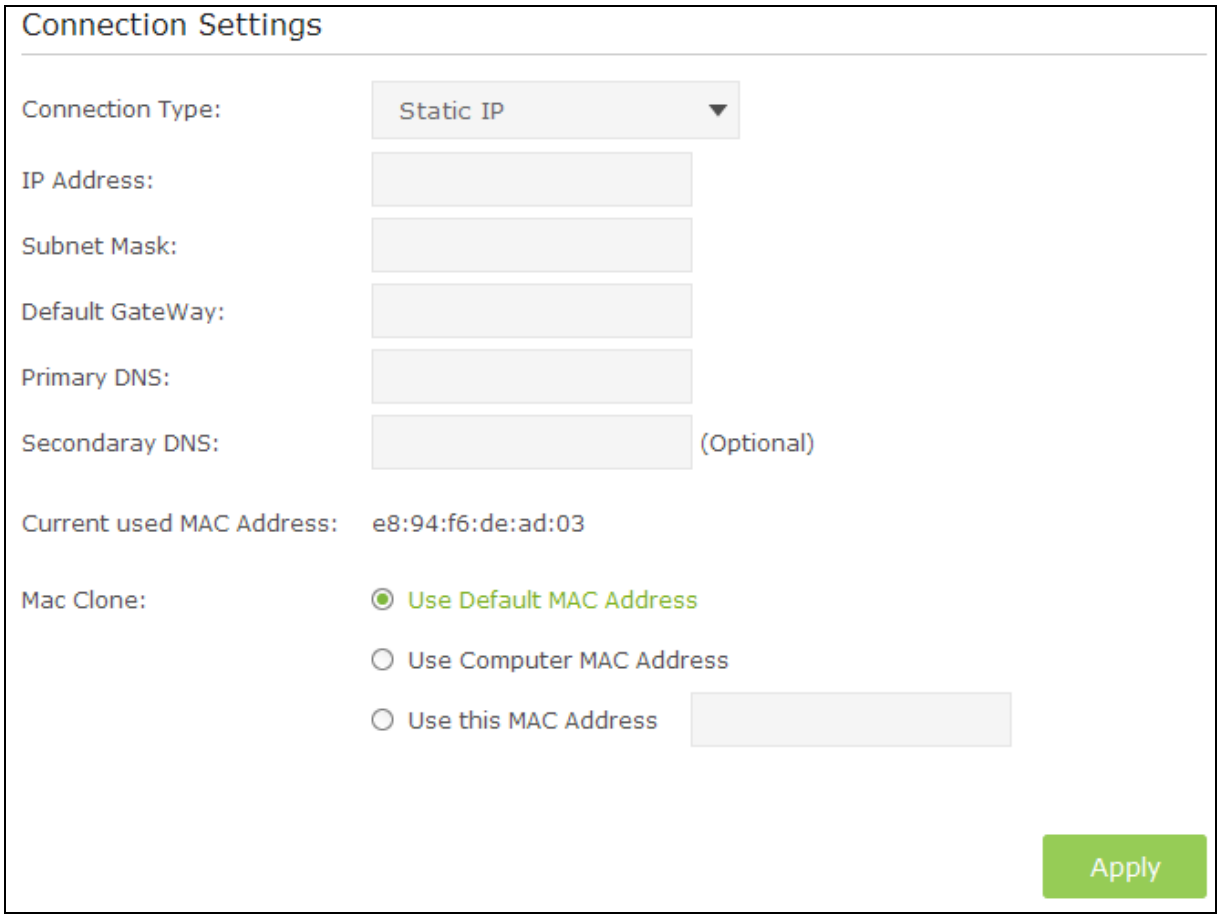


Figure 5-7 WAN - Static IP

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Primary DNS/ Secondary DNS -** Here you can set DNS Server (at least one) manually. The Route will use this DNS Server for priority.
- **Current used MAC Address -** This field displays the current MAC address of the Internet port.
- **MAC Clone -** You can select one of below methods to change MAC address for this WAN Interface depend on your needs. If you select **Use this MAC Address**, you can enter the MAC Address you want to change.

Click the **Apply** button to save the settings.

3) L2TP(Dynamic IP)

Choose **L2TP(Dynamic IP)** in the drop-down list if your ISP provides L2TP(Dynamic IP) information to you. You should set User name, Password and Server IP Address/Name in the screen below.

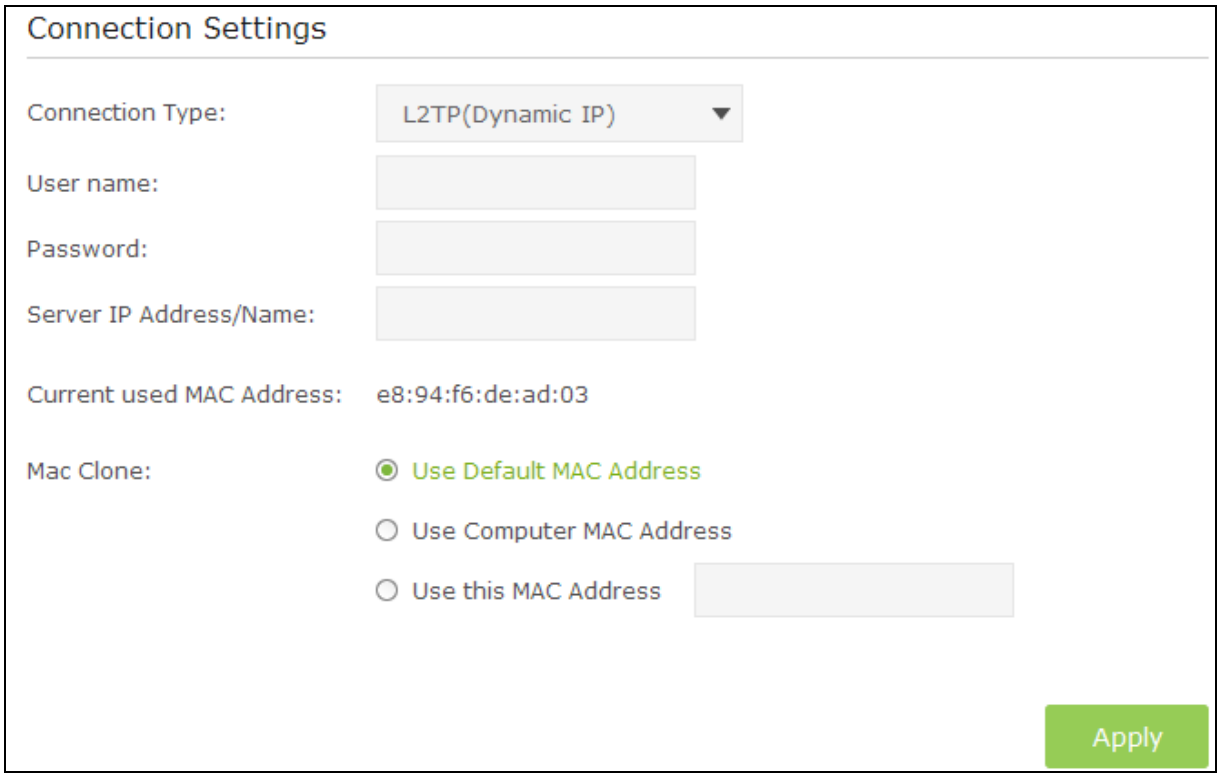


Figure 5-8

- **User name/Password -** Enter the **Username** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.
- **Server IP Address/Name -** Enter the server IP address or domain name provided by your ISP. If you have difficulty with this process, please contact your ISP.
- **Current used MAC Address -** This field displays the current MAC address of the Internet port.
- **MAC Clone -** You can select one of below methods to change MAC address for this WAN Interface depend on your needs. If you select **Use this MAC Address**, you can enter the MAC Address you want to change.

Click the **Apply** button to save the settings.

4) L2TP(Static)

Choose **L2TP(Static)** in the drop-down list if your ISP provides L2TP(Static IP) information to you. You should set User name, Password, Server IP Address/Name, IP Address, Subnet Mask and Default Gateway in the screen below.

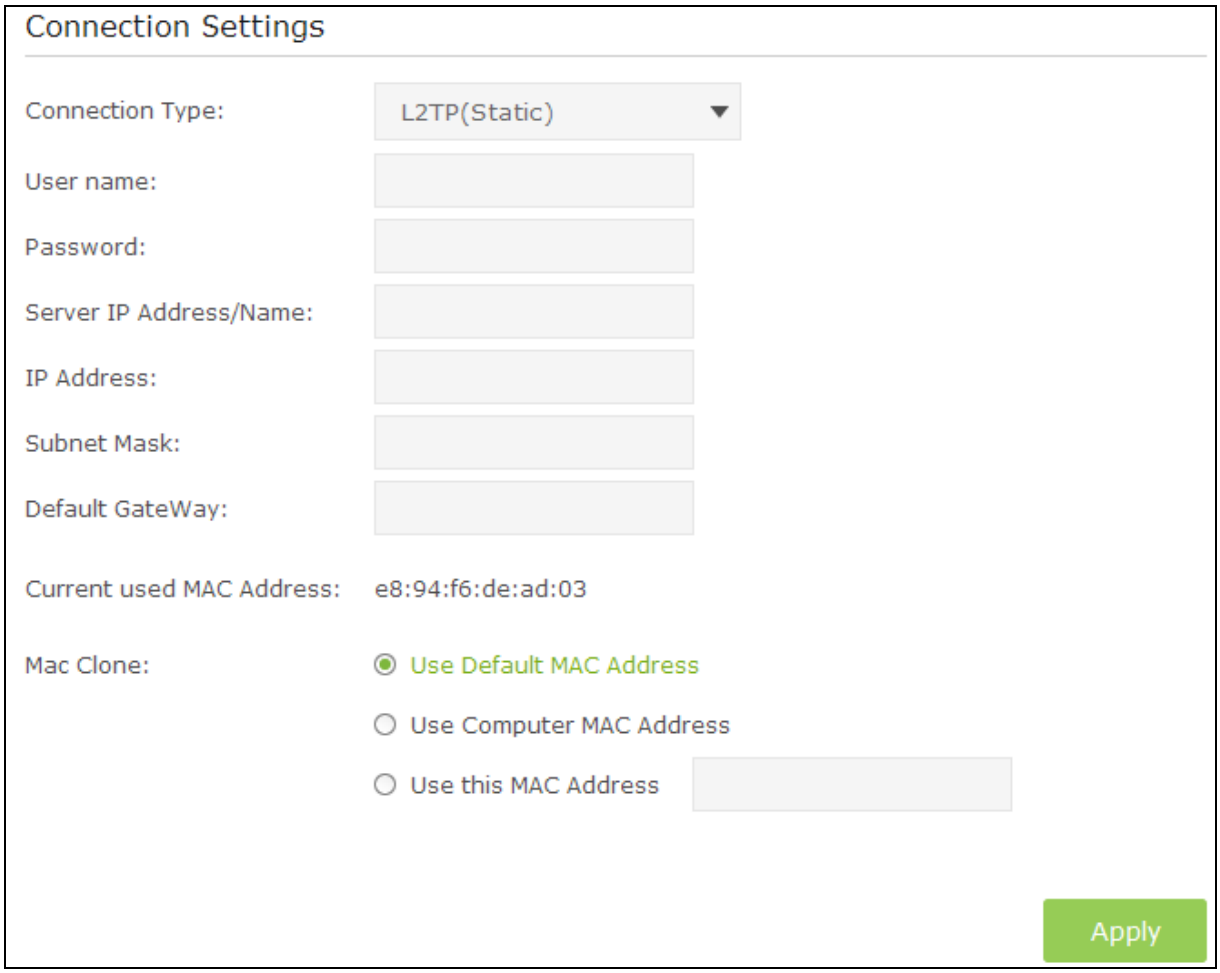


Figure 5-9

- **User name/Password -** Enter the **Username** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.
- **Server IP Address/Name -** Enter the server IP address or domain name provided by your ISP. If you have difficulty with this process, please contact your ISP.
- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Current used MAC Address -** This field displays the current MAC address of the Internet port.
- **MAC Clone -** You can select one of below methods to change MAC address for this WAN Interface depend on your needs. If you select **Use this MAC Address**, you can enter the MAC Address you want to change.

Click the **Apply** button to save the settings.

5.3.2 LAN Settings

Choose "**Advanced→Network→LAN Settings**" menu, and you will see the LAN screen (shown in Figure 5-10). Please configure the parameters for LAN ports according to the descriptions below.

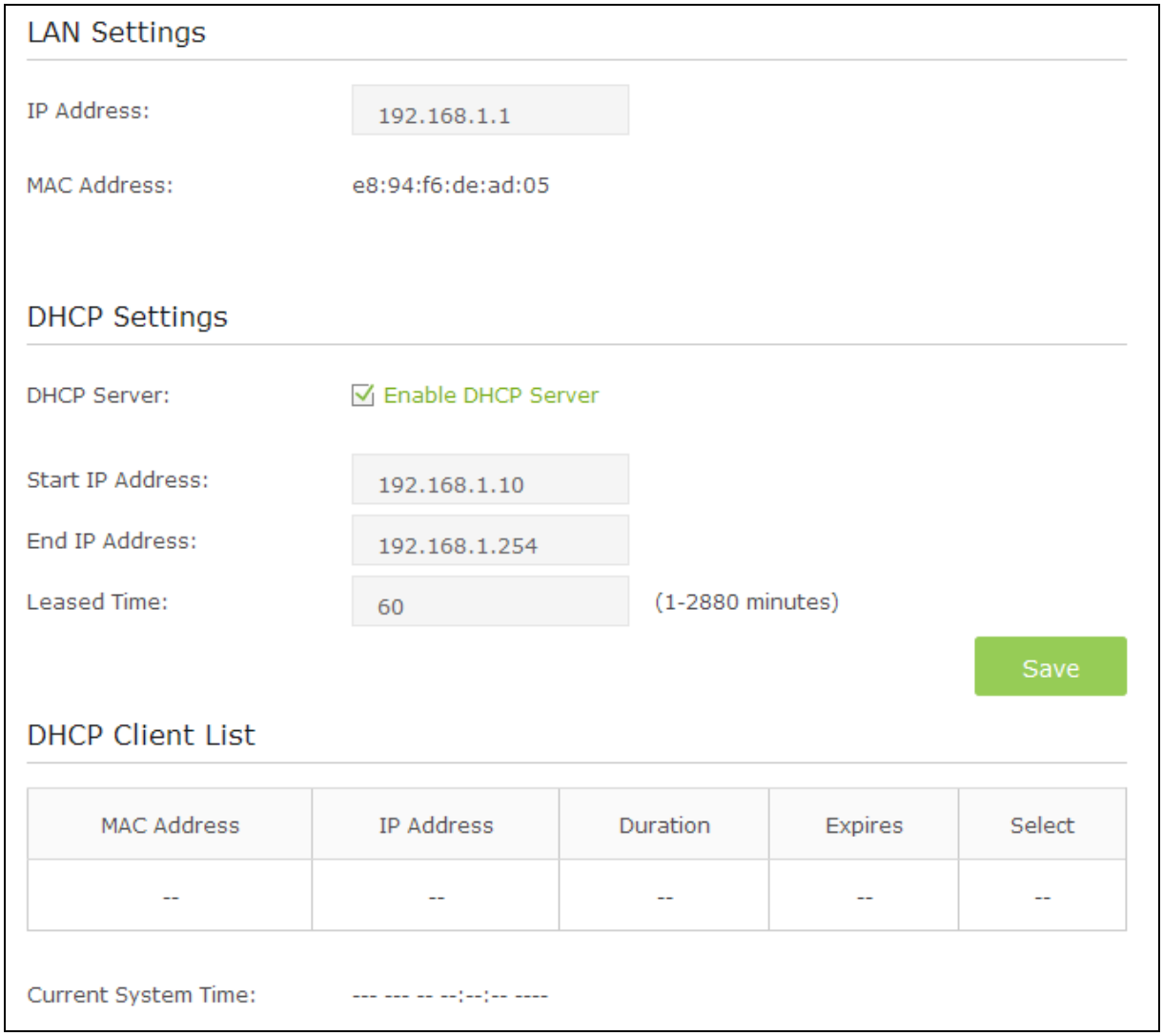


Figure 5-10

LAN Settings:

- **IP Address -** Enter the modem router's local IP Address, then you can access to the Web-based management page via the IP Address, the default value is 192.168.1.1.
- **MAC Address -** The physical address of the modem router, as seen from the LAN. The value can't be changed.

DHCP Settings:

- **DHCP Sever –** Check the box to enable this function. If DHCP Server is enabled, the modem router will work as a DHCP server, which provides the TCP/IP configuration for all the PC(s) that are connected to it on the LAN.
- **MAC Address -** The MAC address of the DHCP client

- **Start IP Address -** Enter a value for the DHCPv6 server to start with when issuing IP addresses.
- **End IP Address -** Enter a value for the DHCPv6 server to end with when issuing IP addresses.
- **Leased Time -** The Leased Time is the amount of time in which a network user will be allowed connection to the modem router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is 60 minutes.

Click the **Save** button to save the settings.

DHCP Clint List:

- **MAC Address -** The MAC address of the DHCP client
- **IP Address -** The IP address that the modem router has allocated to the DHCP client
- **Duration -** Display the total connection time.
- **Expires-** Display the expiration time of the DHCP client leased.
- **Select –** Click the  icon to delete this entry.

5.3.3 IPv6 LAN Settings

Choose "**Advanced→Network→IPv6 LAN Settings**" menu, and you will see the IPv6 LAN screen. Please configure the parameters for IPv6 LAN ports according to the descriptions below.

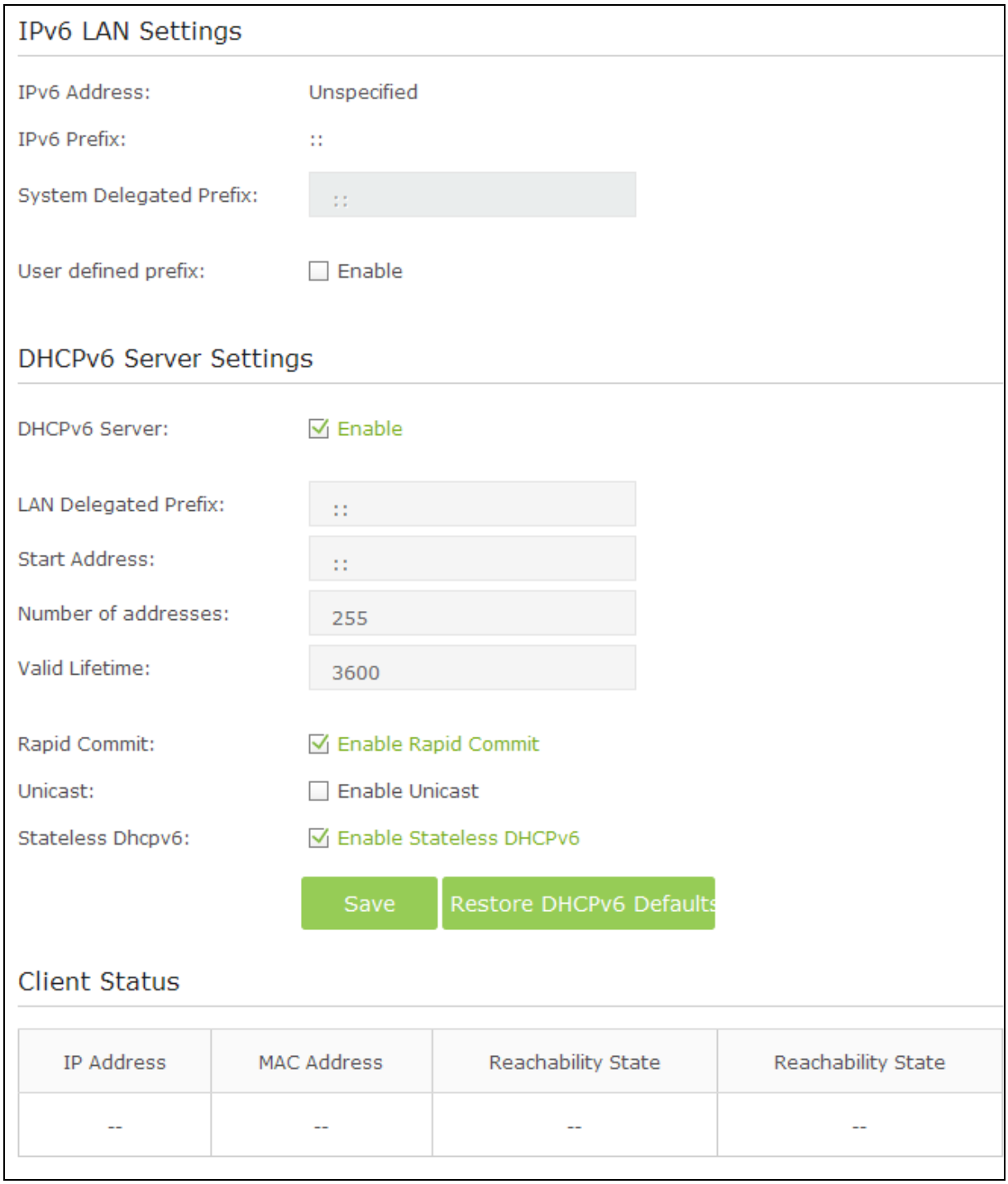


Figure 5-11 IPv6 LAN Settings

IPv6 LAN Settings:

- **IPv6 Address -** Display the modem router's local IPv6 Address.

DHCPv6 Server Settings:

- **DHCPv6 Server –** Check the box to enable this function.
- **Number of addresses –** Enter a value for the DHCPv6 server to start with when issuing IPv6 addresses.
- **Rapid Commit** – Check the box to enable this function.

- **Unicast -** This is disabled by default. The minority of DHCPv6 Server of ISP will not support to enable this. When the modem router is connected right but IPv6 address cannot get, you can select this box.
- **Stateless Dhcpv6 -** Check the box to enable this function.

Client Status:

- **IP Address -** The IP address of the DHCP client
- **MAC Address -** The MAC address of the DHCP client

5.3.4 Dynamic DNS

Choose menu "**Advanced → Network → Dynamic DNS**", and you can configure the Dynamic DNS function.

The modem router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org. The Dynamic DNS client service provider will give you a password or key.

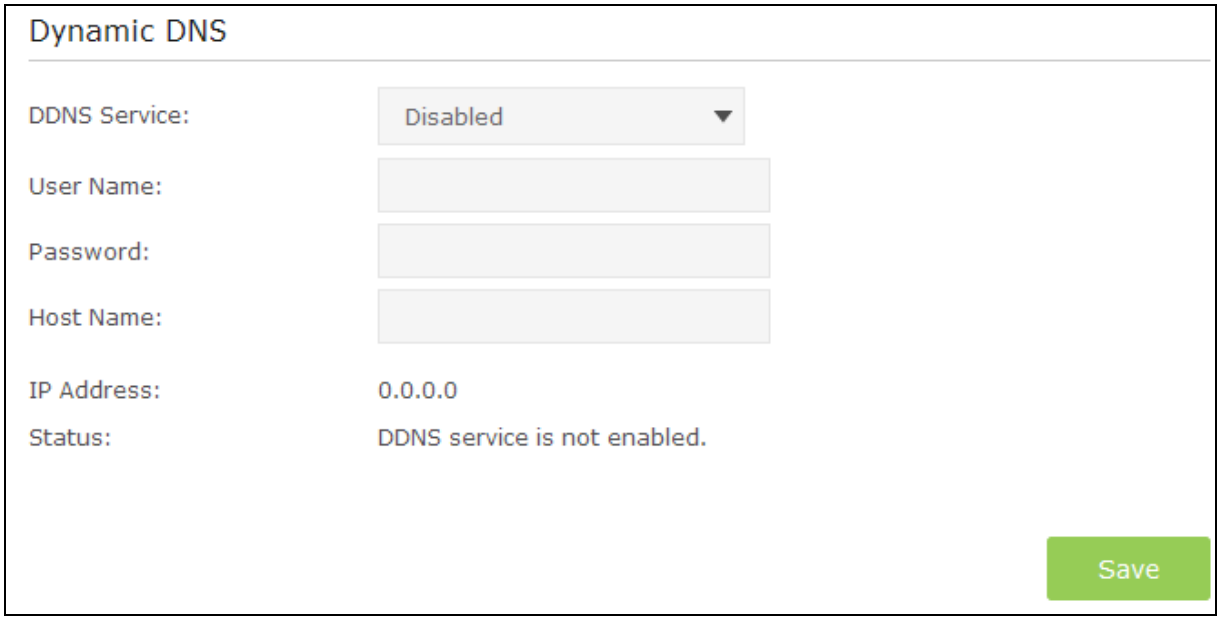


Figure 5-12

- **DDNS Service -** The service provider of DDNS. In this field you could select Disabled, www.DynDns.org or www.noip.net . If you have selected www.DynDns.org or www.noip.net , you need to sign up for DDNS service providers.
- **User Name & Password -** Type the "User Name" and "Password" for your DDNS account.
- **Host Name -** Enter the Domain name you want to set.
- **IP Address –** Display the WAN IP address.

Click the **Save** button to save your settings.

5.3.5 Advanced Routing

Choose "**Advanced** → **Network** → **Advanced Routing**", you can view all the current groups on this page (shown in Figure 5-13).

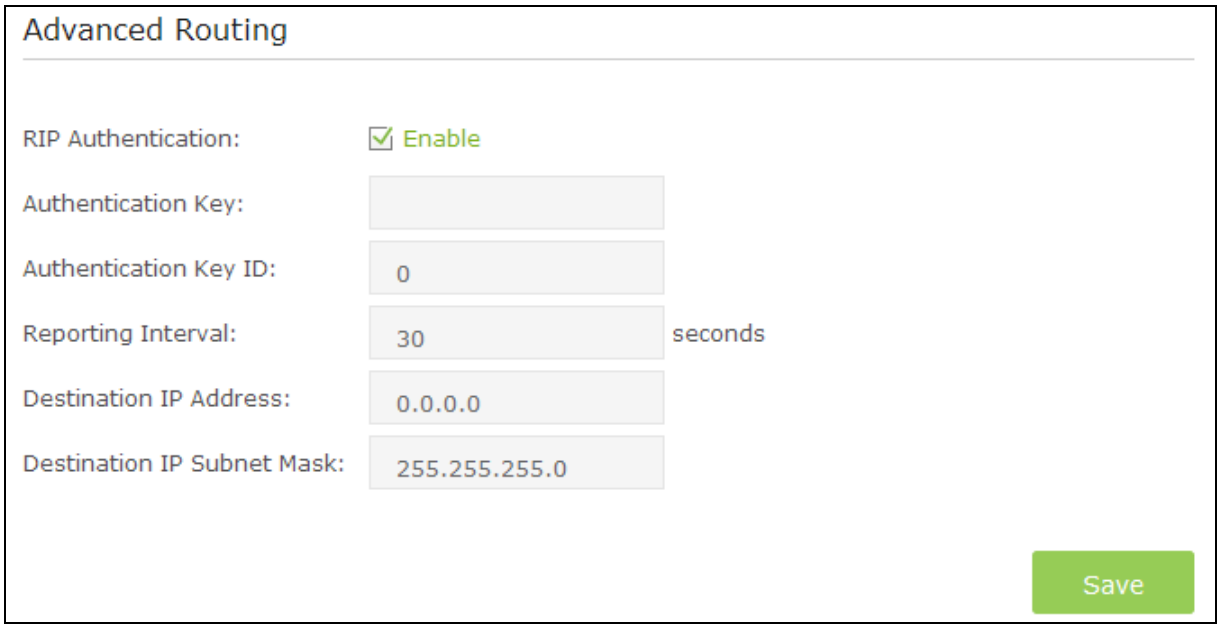
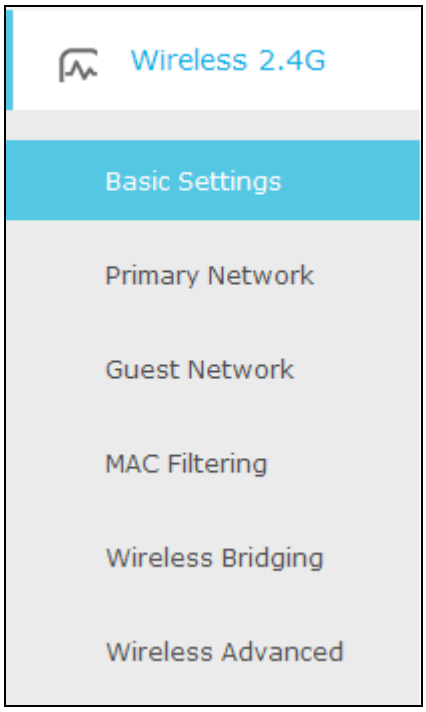


Figure 5-13

- **RIP Authentication –** Check the box to enable the RIP Authentication function.
- **Authentication Key –** Create a key（up to 16 characters）for the RIP authentication.
- **Authentication Key ID -** Create a ID（up to 3 characters） for identity a authentication key.
- **Reporting Interval –** Refer to the update interval for routing information.
- **Destination IP Address –**The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Destination IP Subnet Mask –**The **Destination IP Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.

Click **Save** button to save the settings.

5.4 Wireless 2.4G



Choose menu "**Advanced→Wireless 2.4G**", you will see six submenus under the Wireless menu: **Basic Settings**, **Primary Network, Guest Network**, **MAC Filtering**, **Wireless Bridging** and **Wireless Advanced**. Click any of them, and you will be able to configure the corresponding function.

5.4.1 Basic Settings

Choose menu "**Advanced → Wireless 2.4G → Basic Settings**", you can configure the advanced wireless settings for the wireless 2.4G network.

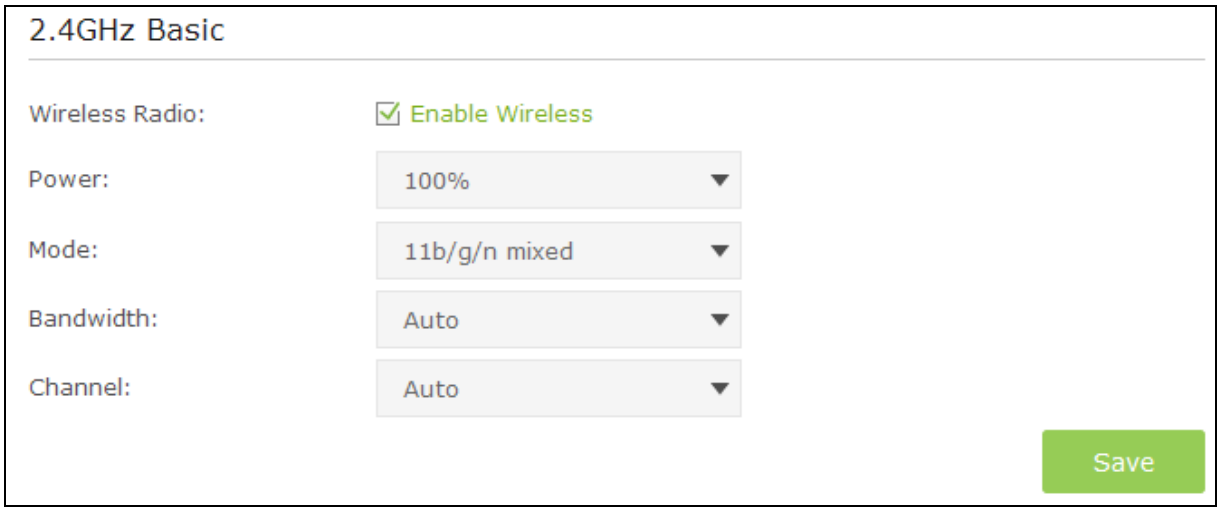


Figure 5-14

- **Wireless Radio –** Check the box to enable the Wireless Radio.

- **Power –** Here you can specify the transmit the power of the modem router. You can select 25%, 50%, 75% and 100% which you would like. 100% is the default setting and is recommended.
- **Mode –** Select the desired mode.

  11b/g mixed: Select if you are using both 802.11b and 802.11g wireless clients.

  11b/g/n mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

  Select the desired wireless mode. It is strongly recommended that you set the Mode to **11b/g/n mixed**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the modem router.
- **BandWidth -** Select the channel width from the drop-down list. The default setting is Auto, which can adjust the channel width for your clients automatically.
- **Channel -** Select the channel you want to use from the drop-down list of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

☞ **Note:**

If **11b/g mixed** is selected in the **Mode** field, the **BandWidth** selecting field value will become 20M hz, and which is unable to be changed.

Click the **Save** button to save the settings.

5.4.2 Primary Network

Choose menu "**Advanced → Wireless 2.4G → Primary Network**", You can configure the wireless 2.4G primary network.

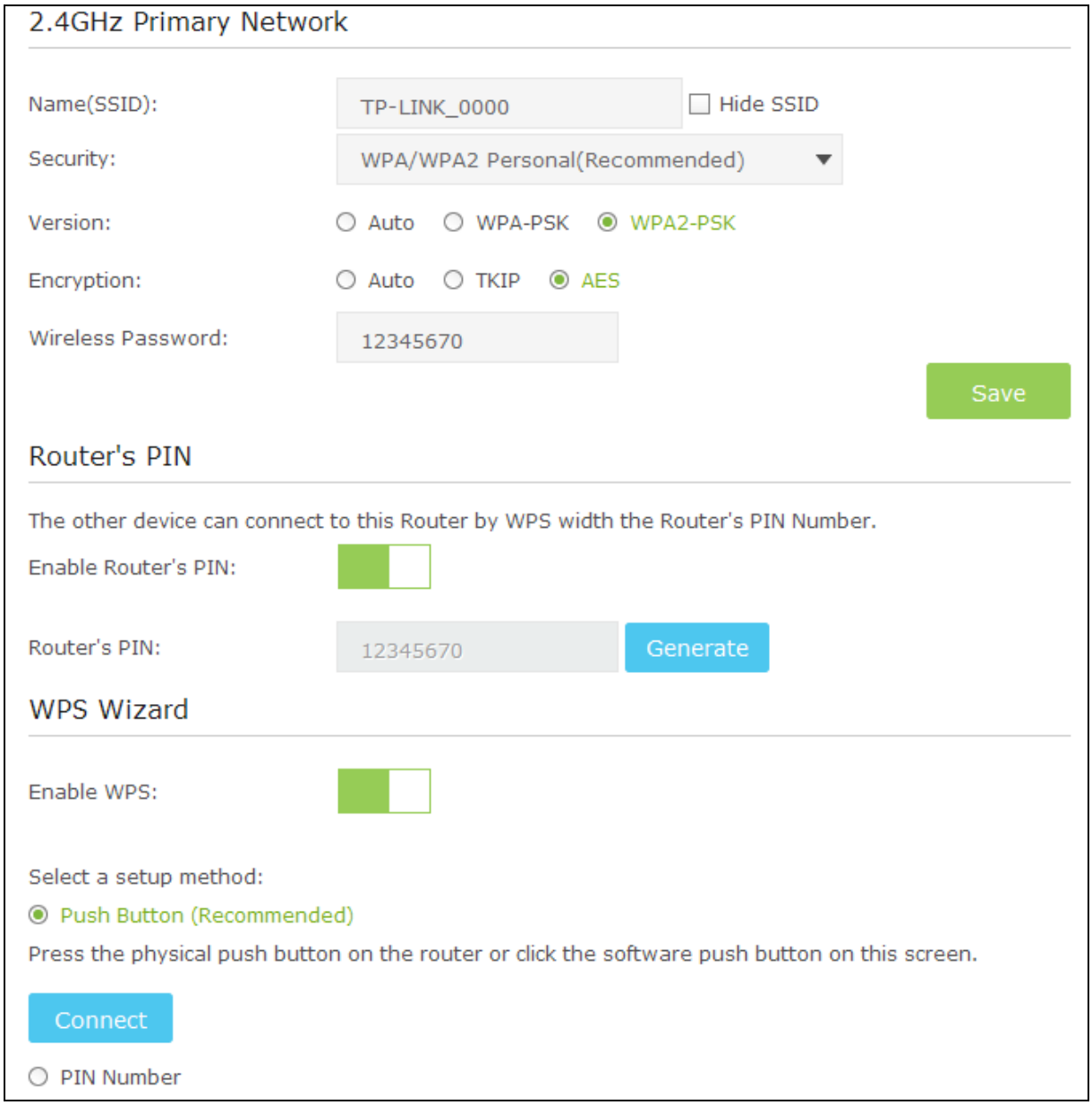


Figure 5-15

2.4GHz Primary Network:

- **Name (SSID) –** Create a name (up to 32 characters) for your 2.4GHz wireless network. The default SSID is set to be TP-LINK_XXXX.
- **Hide SSID –** If you want to hide the SSID of your wireless network from the Wi-Fi network, you should check the box.
- **Security –** There are four wireless security modes supported by the modem router: **No Security**, **WPA/WPA2 Personal (Recommended)**, **WPA/WPA2 Enterprise**, **WEP**. You can choose one of them from the drop-down list.

1) **No Security:** If you do not want to use wireless security, choose **No Security**. But it's recommended to use wireless security.

2) **WPA-PSK/WPA2-PSK Personal(Recommended):**

- **Version –**You can choose the version of the WPA-PSK/WPA2-PSK security by selecting **Auto, WPA-PSK** or **WPA2-PSK**. The default setting is **WPA2-PSK**.
- **Encryption –** You can choose the encryption by selecting **Auto, TKIP** or **AES**. The default setting is **AES**.
- **Wireless Password –** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the back of the modem router.

3) WPA/WPA2 Enterprise:

- **Version –**You can choose the version of the WPA/WPA2 Enterprise security by selecting **Auto**, **WPA** or **WPA2**. The default setting is **WPA2**.
- **Encryption –** You can select **Auto, TKIP** or **AES** as Encryption. The default setting is **AES**.
- **RADIUS Server IP:** Enter the IP address of the Radius Server.
- **RADIUS Port:** Enter the port that radius service used.
- **RADIUS Password:** Enter the password for the Radius Server.

4) WEP:

- **Key Selected –** Select one of the four keys from the drop-down list.
- **Key Type –**You can select the WEP key length (64-bit, or 128-bit.) for encryption.

  64-bit: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

  128-bit: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

- **Key Format – ASCII** and **Hexadecimal** formats are provided here. **ASCII** format stands for any combination of keyboard characters in the specified length. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **Key Value -** Enter the WEP key that you create. Make sure these values are identical on all wireless stations in your network.

  ☞ **Note:**

  If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key.

Router's PIN:

- **Enable Router's PIN -** The switch for the Router's PIN. If you turn on this button, the field will become green and other device can connect to this Router by WPS with the Router's PIN Number.
- **Router's PIN -** The current value of the modem router's PIN is displayed here. The default PIN of the modem router can be found in the label.
- **Generate -** Click this button, and then you can get a new random value for the modem router's PIN. You can ensure the network security by generating a new PIN.

☞ **Note:**

You cannot connect other device to this modem router by entering the router's PIN on your client

device if you haven't switch on **Enable Router's PIN**.

WPS Wizard:

- **Select a setup method –** You can select either of **Push Button (Recommended)** or **PIN Number** as the WPS setup method.
- **Push Button (Recommended) –** When you select this method, you can add a new device by pressing the physical button on the router or by clicking the software push **Connect** button on this screen.
- **PIN Number -** When you select this method, you can add a new device by entering the client's PIN in the field and then click **Connect** button.

To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and modem router using either Push Button method or PIN Number method.

Note:

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. Use the WPS Button

Use this method if your client device has a Wi-Fi Protected Setup (WPS) button.

Step 1: Press the physical button on the router (as shown in Figure 5-16) or click the software push button: **Connect** (as shown in Figure 5-17).

Figure 5-16

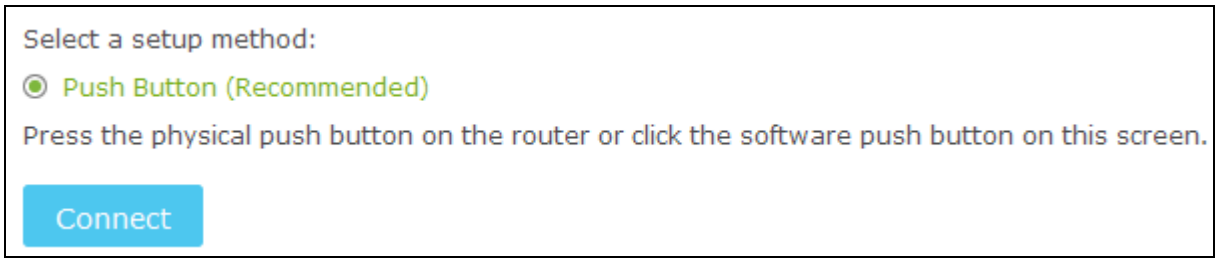


Figure 5-17

Step 2: Press and hold the WPS button of the client device directly.

Step 3: The WPS LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: When the WPS LED is on, the client device has successfully connected to the modem router.

Refer back to your client device or its documentation for further instructions.

II. Enter the client device's PIN on the modem router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 1: Enter the PIN number from the client device in the field, as shown in the following figure. Then click **Connect** button.

Figure 5-18

Step 2: "**Device has been added successfully!**" will appear on the screen, which means the client device has successfully connected to the modem router.

☞ **Note:**

1) The WPS LED on the modem router will light green for five minutes if the device has been successfully added to the network.
2) The WPS function cannot be configured if the **Enable Router's PIN** switch is off. Please make sure the **Enable Router's PIN** switch is on before configuring the WPS.

5.4.3 Guest Network

Choose menu "**Advanced → Wireless 2.4G → Guest Network**", you can configure the advanced settings of your guest network.

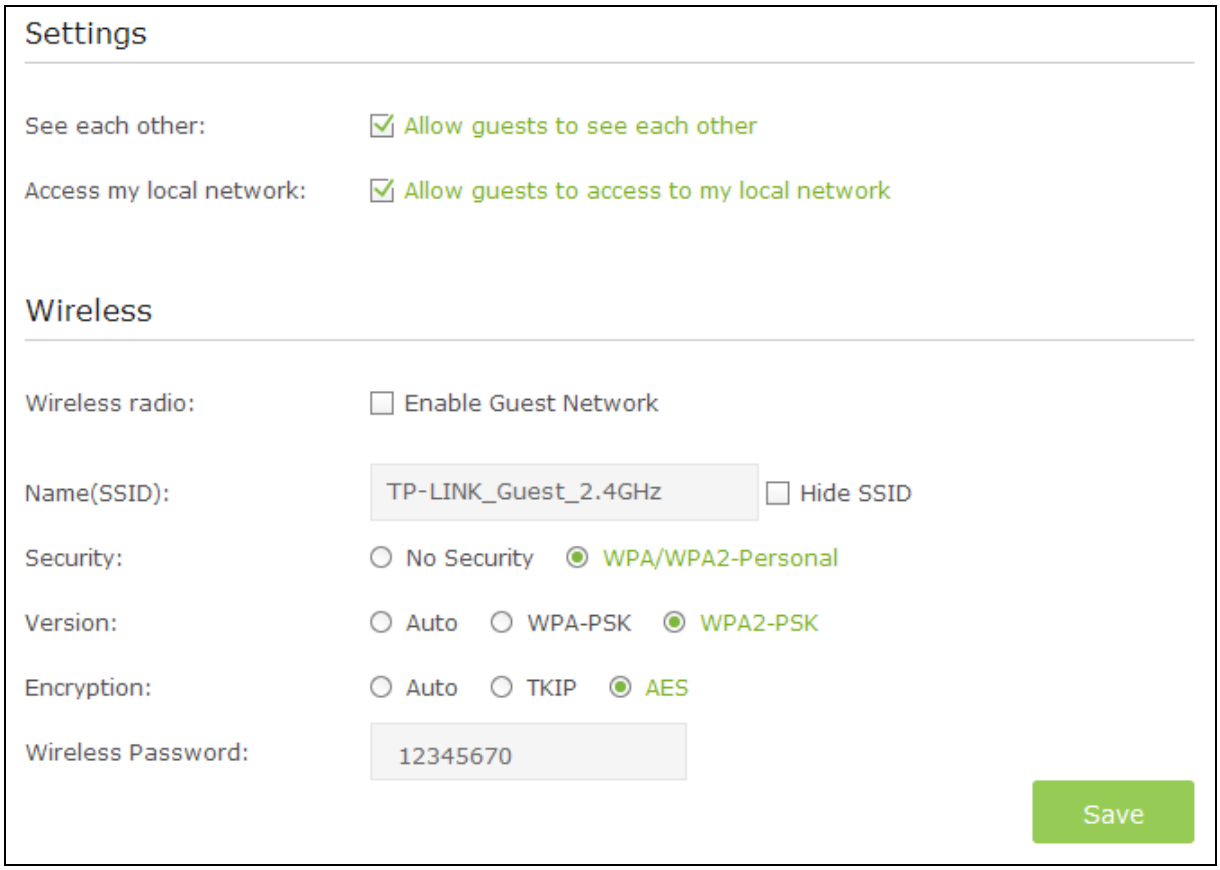


Figure 5-19

Settings:

- **See each other -** If **Allow guests to see each other** is selected, anyone who connects to the guest network can **access** each other.
- **Access my local network -** If **Allow guests to access my local network** is selected, anyone who connects to the guest network has access to your local network, not just Internet access.

Wireless:

- **Wireless radio –** Check the box to enable this function. The guest network function is disabled by default.
- **Name (SSID) -** Create a name for the guest network. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network. The default name is TP-LINK_Guest_2.4GHz. If you want to hide the guest network from the Wi-Fi network, check the **Hide SSID**.
- **Security -** It's strongly recommended to select **WPA/WPA2 Personal**. If you do not want to use wireless security, choose **No Security**.
- **Version -**You can choose the version of the WPA-PSK/WPA2-PSK security by selecting **Auto, WPA-PSK** or **WPA2-PSK**. The default setting is **WPA2-PSK**.
- **Encryption -** You can choose the encryption by selecting **Auto, TKIP** or **AES**.
- **Wireless Password -** Create a password for the guest network. The password must have a minimum of 8 characters in length.

Click **Save** button to save the settings.

5.4.4 Wireless Advanced

Choose menu "**Advanced → Wireless 2.4G → Wireless Advanced**", you can configure the advanced settings of your wireless network.

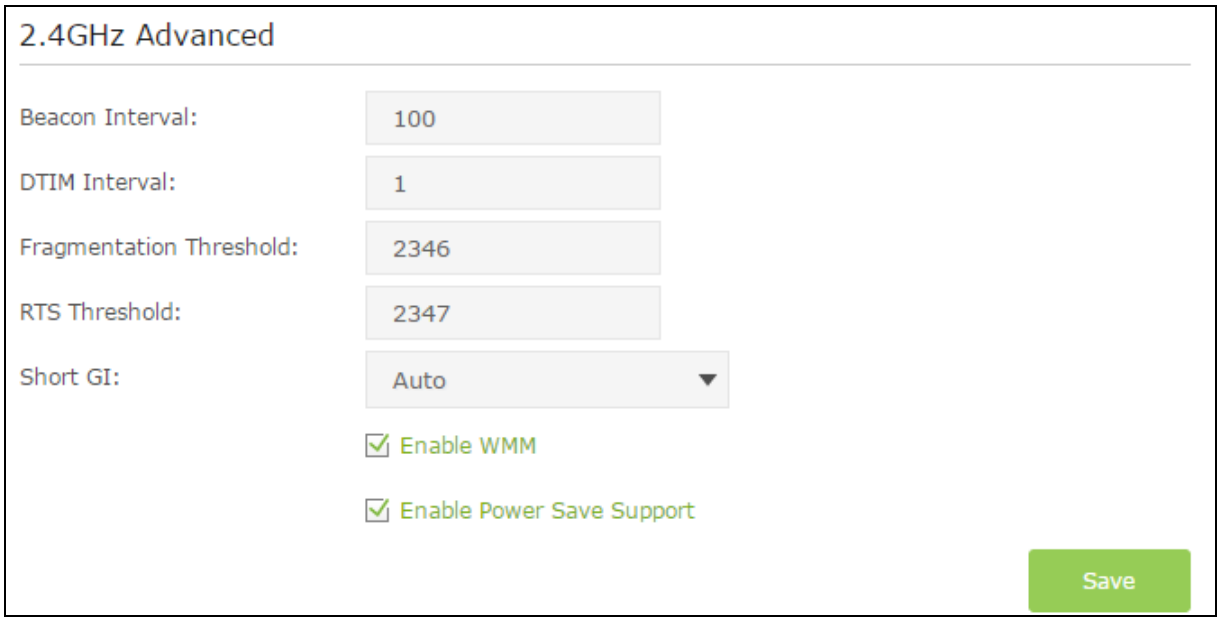


Figure 5-20

2.4GHz Advanced:

- **Beacon Interval -** Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the modem router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the modem router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the modem router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.
- **Short GI Feature -** This function is recommended for it will increase the data capacity by reducing the guard interval time. Short GI is enabled by default.
- **Enable WMM –** Check the box to enable this function. WMM function can guarantee the packets with high-priority messages being transmitted preferentially, which is strongly recommended. It is enabled by default.

- **Enable Power Save Support -** Check the box to enable this function. This function can make the wireless client has only antenna is in working condition, and the remaining antennas are dormant, so as to achieve the purpose of saving power.

Click the **Save** button to save the settings.

5.4.5 MAC Filtering

Choose menu "**Advanced → Wireless 2.4GHz → MAC Filtering**", you can control the wireless access by configuring the **MAC Filtering** function, shown in Figure 5-21.

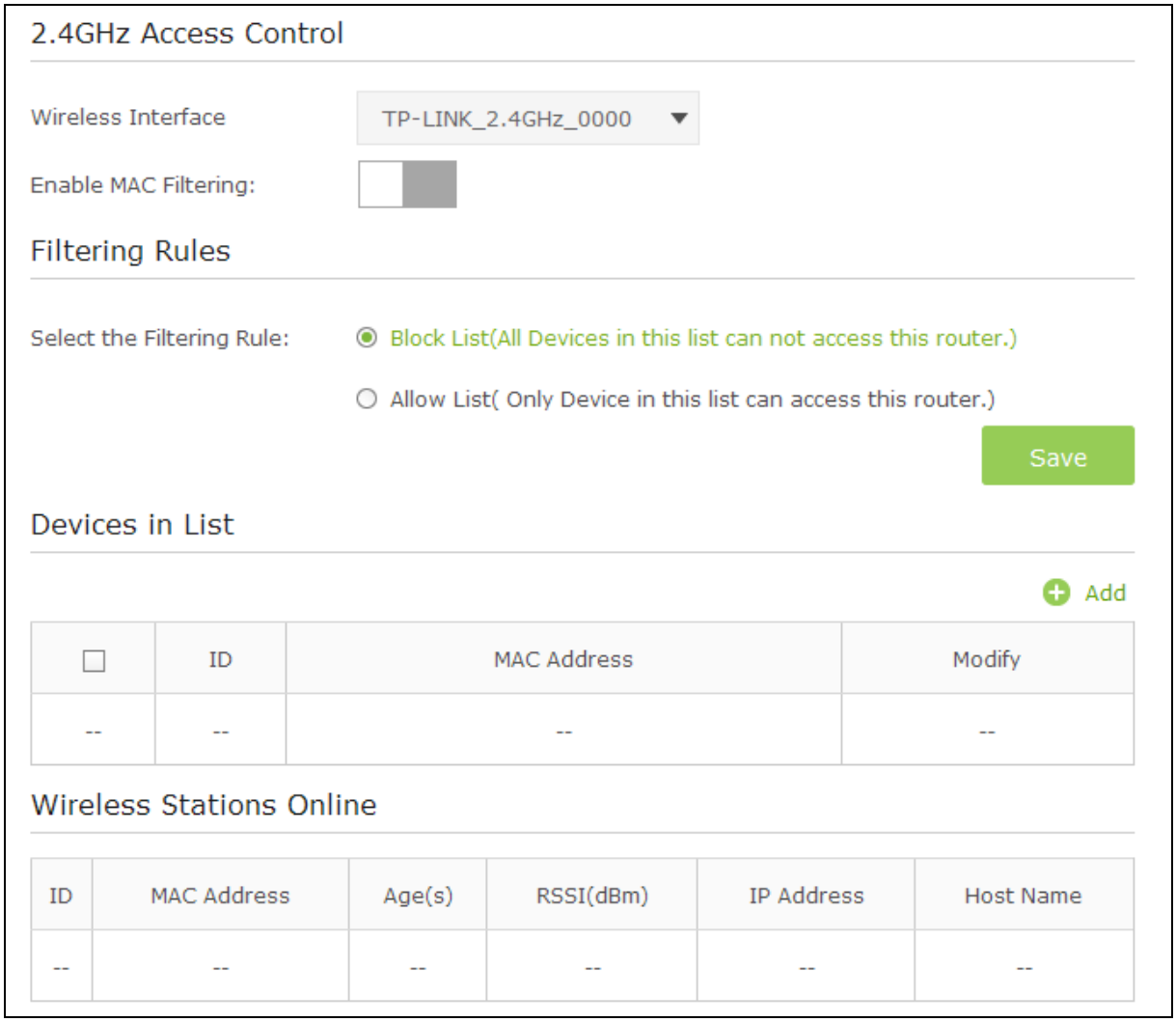


Figure 5-21 Wireless 2.4GHz – MAC Filering

2.4GHz Access Control:

- **Wireless Interface -** Select an available wireless interface from the drop-down list.
- **Enable MAC Filtering-** The switch for the MAC Filtering. If you turn on this button, the field will become green and you can filter wireless users by MAC Address.

Filtering Rules:

- **Select the Filtering Rule -** You can select either of **Block List** or **Allow List** as the MAC filtering rule.

Click the **Save** button to save the settings.

Devices in List:

- **Add -** You can add a new device for the MAC Filtering rule by clicking Add button.
- **MAC Address -** This field displays the MAC address of the wireless station that cannot access this router/can access this router.
- **Modify -** Click the icon to delete this entry.

To add a MAC Address Filtering entry:

1. Click Add button, then you will see a setting page.
2. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.

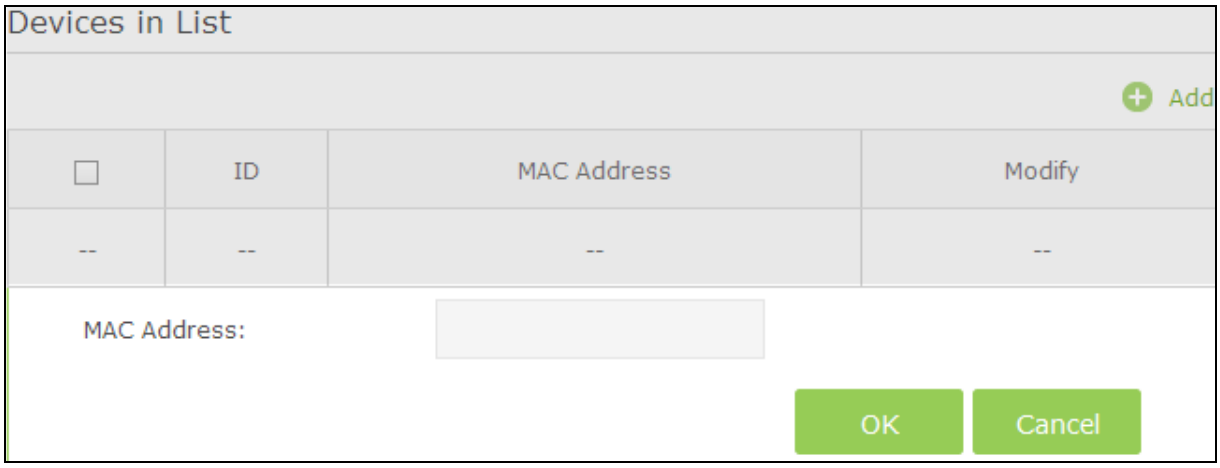


Figure 5-22

3. Click the **OK** button to save this entry. If you do not want to save this entry, click the **Cancel** button.

For example: If you desire that the wireless station A with MAC address 00:1D:0F:11:22:33 and the wireless station B with MAC address 00:0A:EB:00:07:5F are able to access the modem router, but all the other wireless stations cannot access the modem router, you can configure the **MAC Filtering** settings by following these steps:

1. Switch on the **Enable MAC Filtering** button to enable this function.
2. Select the **White List** for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the Add button.
   1) Enter the MAC address 00:1D:0F:11:22:33/00:0A:EB:00:07:5F in the **MAC Address** field.
   2) Click the **OK** button.

The filtering rules that configured should be similar to the following figure:

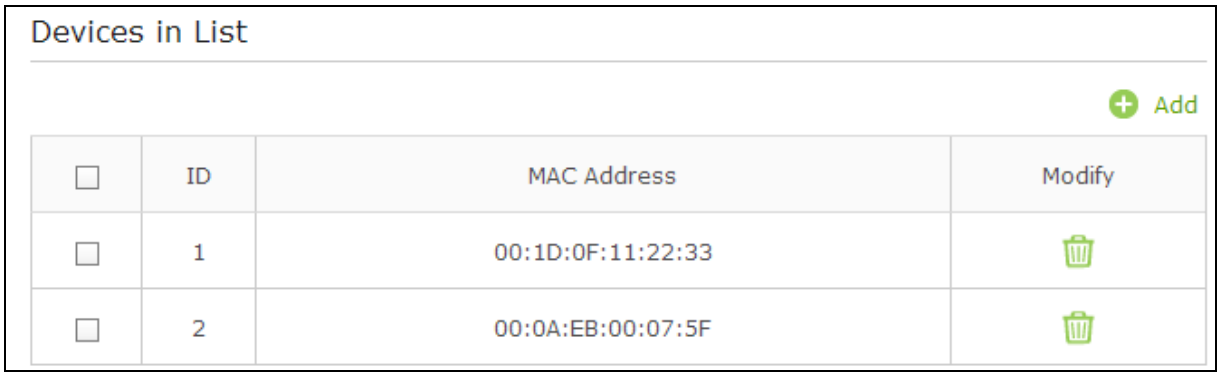


Figure 5-23

Wireless Stations Online:

- **MAC Address -** The MAC address of the wireless station online.
- **Age(s) –** Display the duration time of wireless station online.
- **RSSI(dBm) –** Refers to the Received Signal Strength Indication.
- **IP Address-** The IP address of the wireless station online.
- **Host Name –** Display the host name of the wireless station.

5.4.6 Wireless Bridging

Choose menu "**Advanced → Wireless 2.4G → Wireless Bridging**". With this function, the modem router can bridge more WLANs.

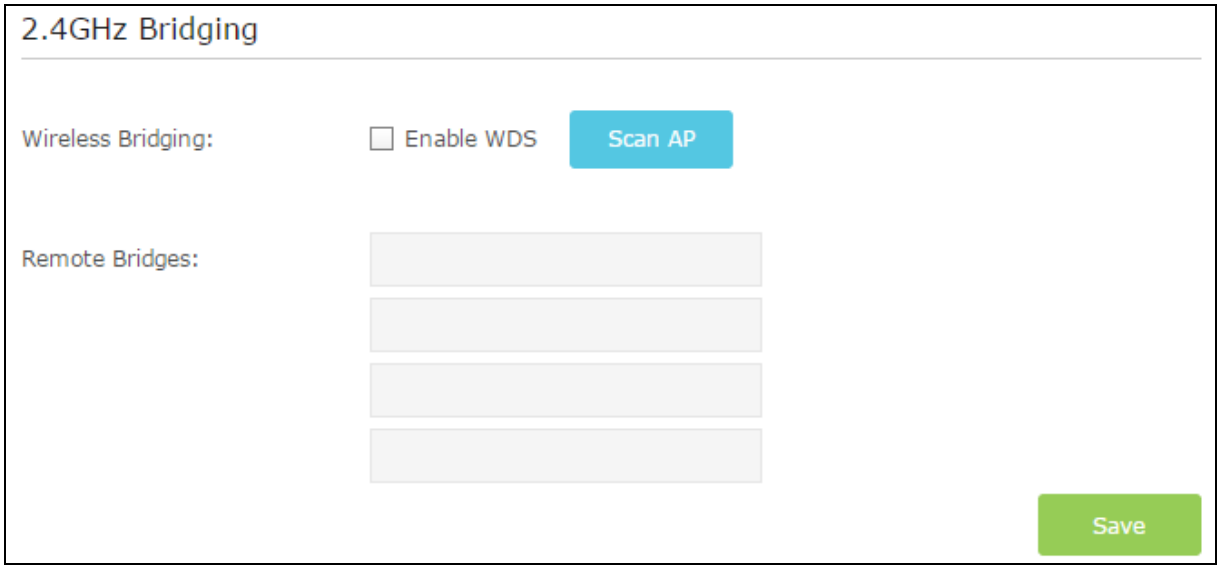
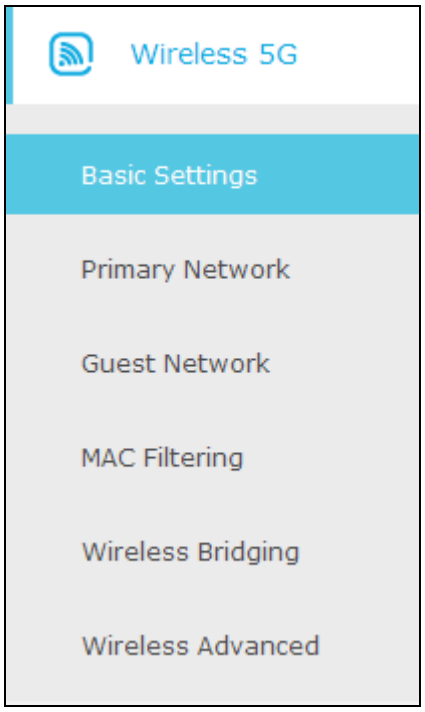


Figure 5-24

- **WDS Bridging -** With this function, the modem router can bridge more WLANs. If you check the **Enable WDS**, you can click the **Scan AP** button to scan the nearby wireless access points.
- **Remote Bridges –** Enter the MAC address the AP your modem router is going to connect to as a client. You can also use the Scan AP function to select the BSSID to join.

Click the **Save** button to save the settings.

5.5 Wireless 5G



Choose menu "**Advanced→Wireless 5G**", you will see six submenus under the Wireless menu: **Basic Settings**, **Primary Network, Guest Network**, **MAC Filtering**, **Wireless Bridging** and **Wireless Advanced**. Click any of them, and you will be able to configure the corresponding function.

5.5.1 Basic Settings

Choose menu "**Advanced → Wireless 5G → Basic Settings**", you can configure the advanced wireless settings for the wireless 5G network.

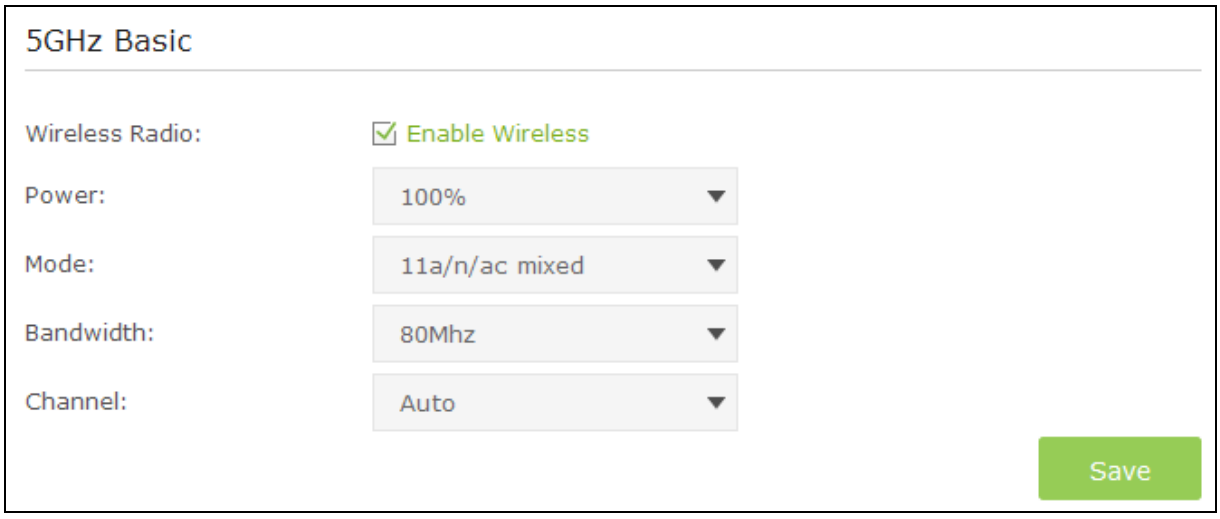


Figure 5-25

- **Wireless Radio –** Check the box to enable the Wireless Radio.

- **Power –** Here you can specify the transmit the power of the modem router. You can select 25%, 50%, 75% and 100% which you would like. 100% is the default setting and is recommended.
- **Mode –** Select the desired mode.

  11a: Select if you are using 802.11a wireless clients.

  11a/n mixed: Select if you are using a mix of 802.11a and 11n wireless clients.

  Select the desired wireless mode. It is strongly recommended that you set the Mode to **11b/g/n mixed**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the modem router.

  11a/n mixed: Select if you are using a mix of 802.11a and 11n wireless clients.

  Select the desired wireless mode. It is strongly recommended that you set the Mode to **11b/g/ac mixed**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the modem router.
- **BandWidth -** Select the channel width from the drop-down list. The default setting is Auto, which can adjust the channel width for your clients automatically.
- **Channel -** Select the channel you want to use from the drop-down list of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

☞ **Note:**

If **11b/g mixed** is selected in the **Mode** field, the **BandWidth** selecting field value will become 20M hz, and which is unable to be changed.

Click the **Save** button to save the settings.

5.5.2 Primary Network

Choose menu "**Advanced → Wireless 5G → Primary Network**", You can configure the wireless 5G primary network.

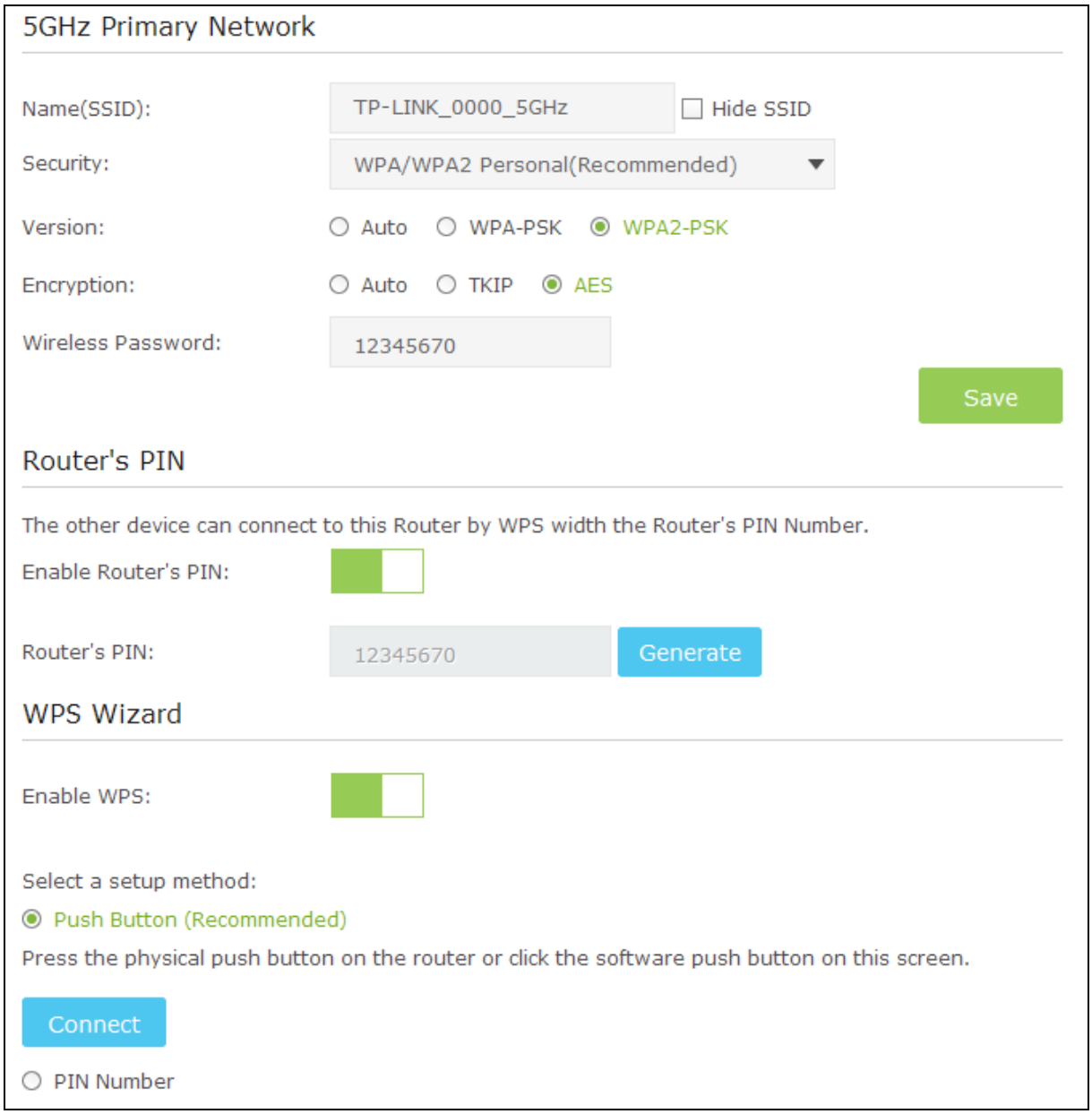


Figure 5-26

2.4GHz Primary Network:

- **Wireless Radio –** Check the box to enable the Wireless Radio.
- **Name (SSID) –** Create a name (up to 32 characters) for your 5GHz wireless network. The default SSID is set to be TP-LINK_XXXX _5GHz.
- **Hide SSID –** If you want to hide the SSID of your wireless network from the Wi-Fi network, you should check the box.
- **Security –** There are four wireless security modes supported by the modem router: **No Security**, **WPA/WPA2 Personal (Recommended)**, **WPA/WPA2 Enterprise**, **WEP**. You can choose one of them from the drop-down list.

5) **No Security:** If you do not want to use wireless security, choose **No Security**. But it's recommended to use wireless security.

6) **WPA-PSK/WPA2-PSK Personal(Recommended):**

- **Version –**You can choose the version of the WPA-PSK/WPA2-PSK security by selecting **Auto, WPA-PSK** or **WPA2-PSK**. The default setting is **WPA2-PSK**.
- **Encryption –** You can choose the encryption by selecting **Auto, TKIP** or **AES**. The default setting is **AES**.
- **Wireless Password –** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the back of the modem router.

7) WPA/WPA2 Enterprise:

- **Version –**You can choose the version of the WPA/WPA2 Enterprise security by selecting **Auto**, **WPA** or **WPA2**. The default setting is **WPA2**.
- **Encryption –** You can select **Auto, TKIP** or **AES** as Encryption. The default setting is **AES**.
- **RADIUS Server IP:** Enter the IP address of the Radius Server.
- **RADIUS Port:** Enter the port that radius service used.
- **RADIUS Password:** Enter the password for the Radius Server.

8) WEP:

- **Key Selected –** Select one of the four keys from the drop-down list.
- **Key Type –**You can select the WEP key length (64-bit, or 128-bit.) for encryption.

  64-bit: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

  128-bit: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

- **Key Format – ASCII** and **Hexadecimal** formats are provided here. **ASCII** format stands for any combination of keyboard characters in the specified length. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **Key Value -** Enter the WEP key that you create. Make sure these values are identical on all wireless stations in your network.

  ☞ **Note:**

  If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key.

Router's PIN:

- **Enable Router's PIN -** The switch for the Router's PIN. If you turn on this button, the field will become green and other device can connect to this Router by WPS with the Router's PIN Number.
- **Router's PIN -** The current value of the modem router's PIN is displayed here. The default PIN of the modem router can be found in the label.
- **Generate -** Click this button, and then you can get a new random value for the modem router's PIN. You can ensure the network security by generating a new PIN.

☞ **Note:**

You cannot connect other device to this modem router by entering the router's PIN on your client

device if you haven't switch on **Enable Router's PIN**.

WPS Wizard:

- **Select a setup method –** You can select either of **Push Button (Recommended)** or **PIN Number** as the WPS setup method.
- **Push Button (Recommended) –** When you select this method, you can add a new device by pressing the physical button on the router or by clicking the software push **Connect** button on this screen.
- **PIN Number -** When you select this method, you can add a new device by entering the client's PIN in the field and then click **Connect** button.

To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and modem router using either Push Button method or PIN Number method.

Note:

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

III. Use the WPS Button

Use this method if your client device has a Wi-Fi Protected Setup (WPS) button.

Step 5: Press the physical button on the router (as shown in Figure 5-27) or click the software push button: **Connect** (as shown in Figure 5-28).

Figure 5-27

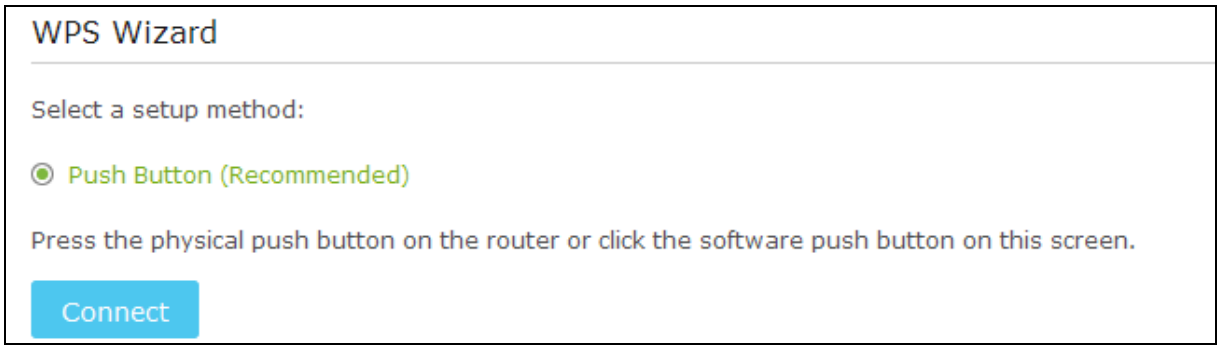


Figure 5-28

Step 6: Press and hold the WPS button of the client device directly.

Step 7: The WPS LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 8: When the WPS LED is on, the client device has successfully connected to the modem router.

Refer back to your client device or its documentation for further instructions.

IV. Enter the client device's PIN on the modem router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 3: Enter the PIN number from the client device in the field, as shown in the following figure. Then click **Connect** button.

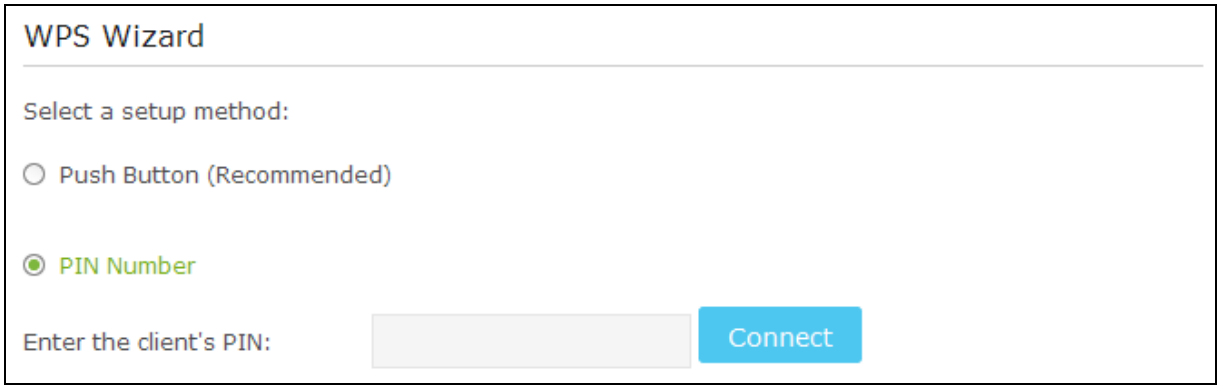


Figure 5-29

Step 4: "**Device has been added successfully!**" will appear on the screen, which means the client device has successfully connected to the modem router.

Note:

1) The WPS LED on the modem router will light green for five minutes if the device has been successfully added to the network.

2) The WPS function cannot be configured if the **Enable Router's PIN** switch is off. Please make sure the **Enable Router's PIN** switch is on before configuring the WPS.

5.5.3 Guest Network

Choose menu "**Advanced→ Wireless 5G → Guest Network**", you can configure the advanced settings of your guest network.

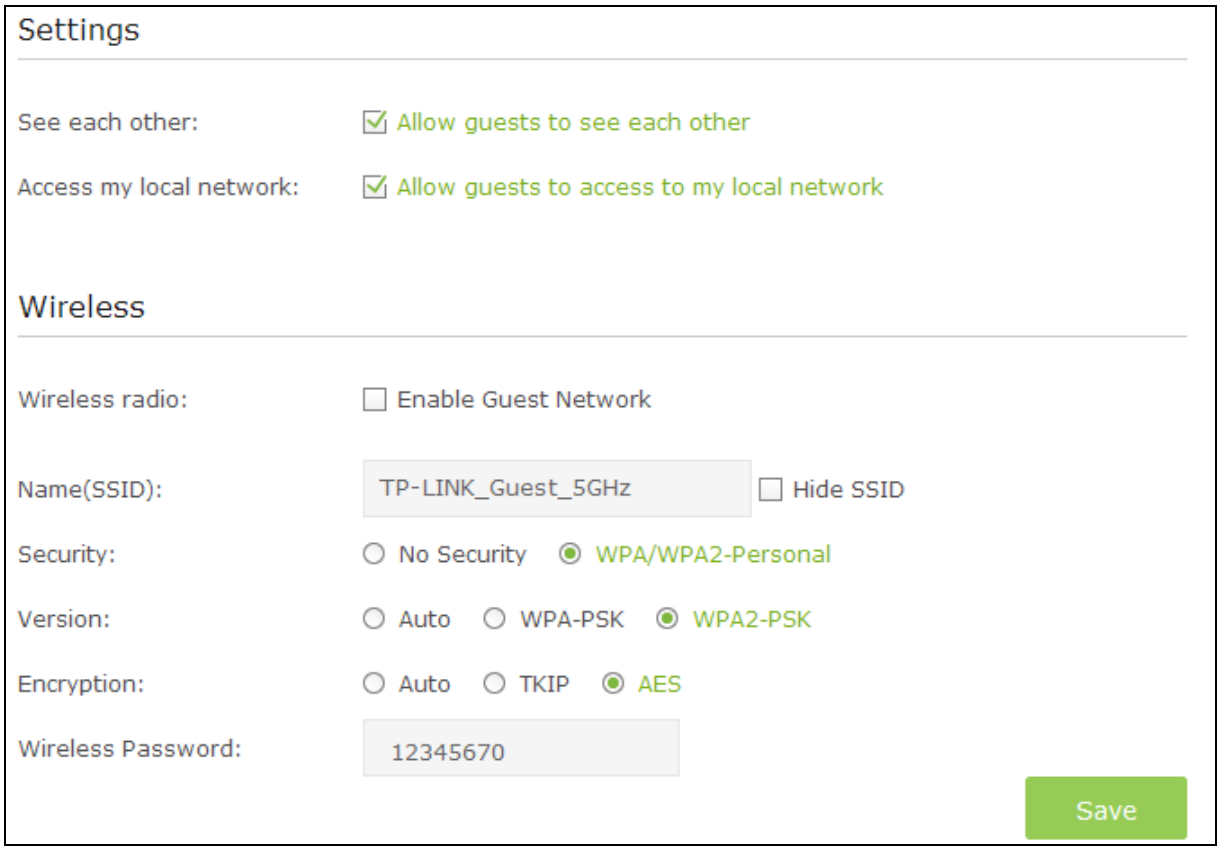


Figure 5-30

Settings:

- **See each other -** If **Allow guests to see each other** is selected, anyone who connects to the guest network can **access** each other.
- **Access my local network -** If **Allow guests to access my local network** is selected, anyone who connects to the guest network has access to your local network, not just Internet access.

Wireless:

- **Wireless radio –** Check the box to enable this function. The guest network function is disabled by default.
- **Name (SSID) -** Create a name for the guest network. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network. The default name is TP-LINK_Guest_5GHz. If you want to hide the guest network from the Wi-Fi network, check the **Hide SSID**.
- **Security -** It's strongly recommended to select **WPA/WPA2 Personal**. If you do not want to use wireless security, choose **No Security**.
- **Version -**You can choose the version of the WPA-PSK/WPA2-PSK security by selecting **Auto, WPA-PSK** or **WPA2-PSK**. The default setting is **WPA2-PSK**.
- **Encryption -** You can choose the encryption by selecting **Auto, TKIP** or **AES**.
- **Wireless Password -** Create a password for the guest network. The password must have a minimum of 8 characters in length.

Click **Save** button to save the settings.

5.5.4 MAC Filtering

Choose menu "**Advanced → Wireless 5GHz → MAC Filtering**", you can control the wireless access by configuring the **MAC Filtering** function.

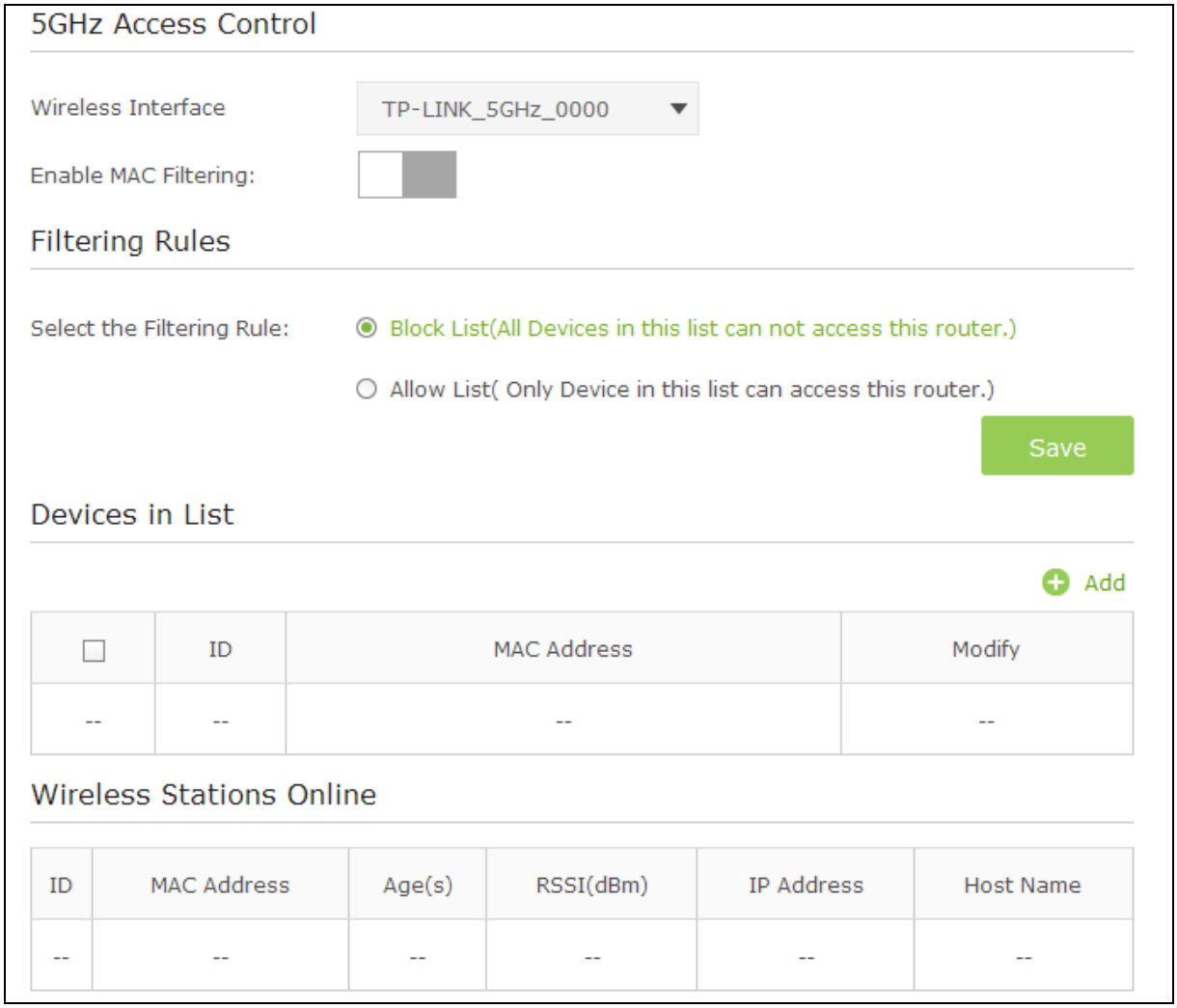


Figure 5-31 Wireless 5GHz – MAC Filering

5GHz Access Control:

- **Wireless Interface -** Select an available wireless interface from the drop-down list.
- **Enable MAC Filtering-** The switch for the MAC Filtering. If you turn on this button, the field will become green and you can filter wireless users by MAC Address.

Filtering Rules:

- **Select the Filtering Rule -** You can select either of **White List** or **Black List** as the MAC filtering rule.

Click the **Save** button to save the settings.

Devices in List:

- **Add -** You can add a new device for the MAC Filtering rule by clicking Add button.

- **MAC Address -** This field displays the MAC address of the wireless station that cannot access this router/can access this router.
- **Modify -** Click the icon to delete this entry.

To add a MAC Address Filtering entry:

1. Click Add button, then you will see a setting page.
2. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.

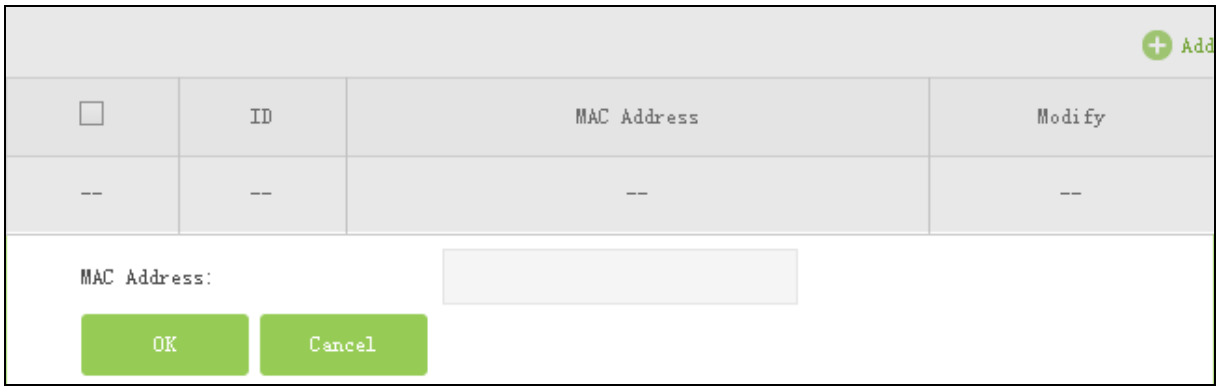


Figure 5-32

3. Click the **OK** button to save this entry. If you do not want to save this entry, click the **Cancel** button.

For example: If you desire that the wireless station A with MAC address 00:1D:0F:11:22:33 and the wireless station B with MAC address 00:0A:EB:00:07:5F are able to access the modem router, but all the other wireless stations cannot access the modem router, you can configure the **MAC Filtering** settings by following these steps:

1. Switch on the **Enable MAC Filtering** button to enable this function.
2. Select the **White List** for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the Add button.
   3) Enter the MAC address 00:1D:0F:11:22:33/00:0A:EB:00:07:5F in the **MAC Address** field.
   4) Click the **OK** button.

The filtering rules that configured should be similar to the following figure:

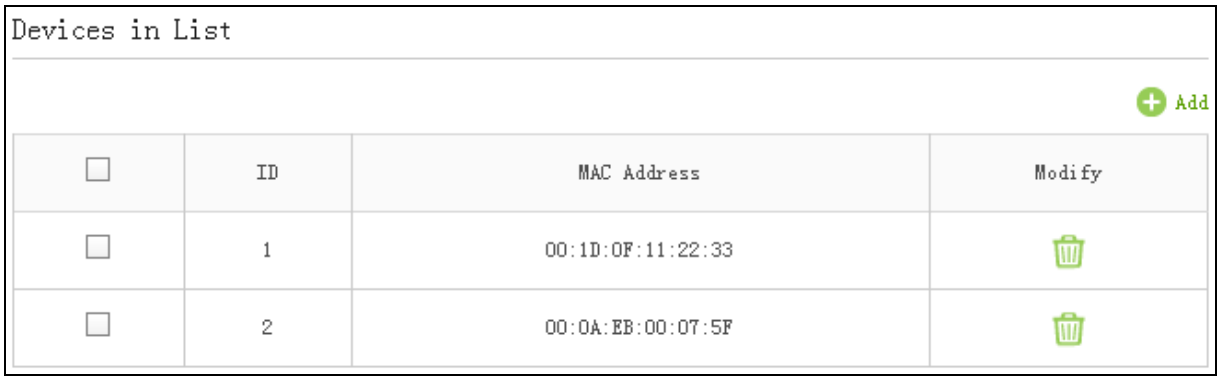
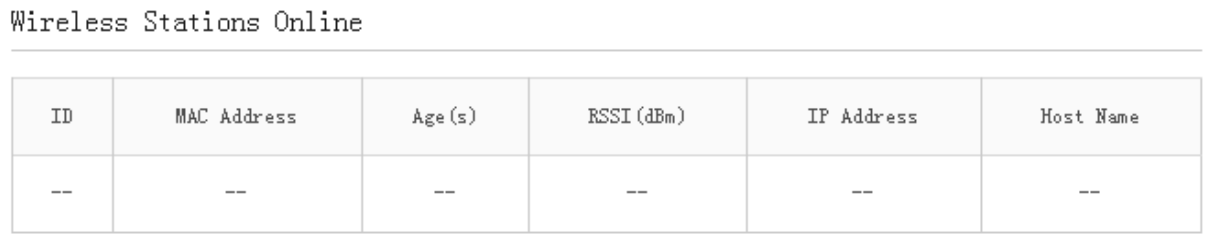


Figure 5-33

Wireless Stations Online:



- **MAC Address -** The MAC address of the wireless station online.
- **Age(s) –** Display the duration time of wireless station online.
- **RSSI(dBm) –** Refers to the Received Signal Strength Indication.
- **IP Address-** The IP address of the wireless station online.
- **Host Name –** Display the host name of the wireless station.

5.5.5 Wireless Bridging

Choose menu "**Advanced → Wireless 5G → Wireless Bridging**". With this function, the modem router can bridge more WLANs.

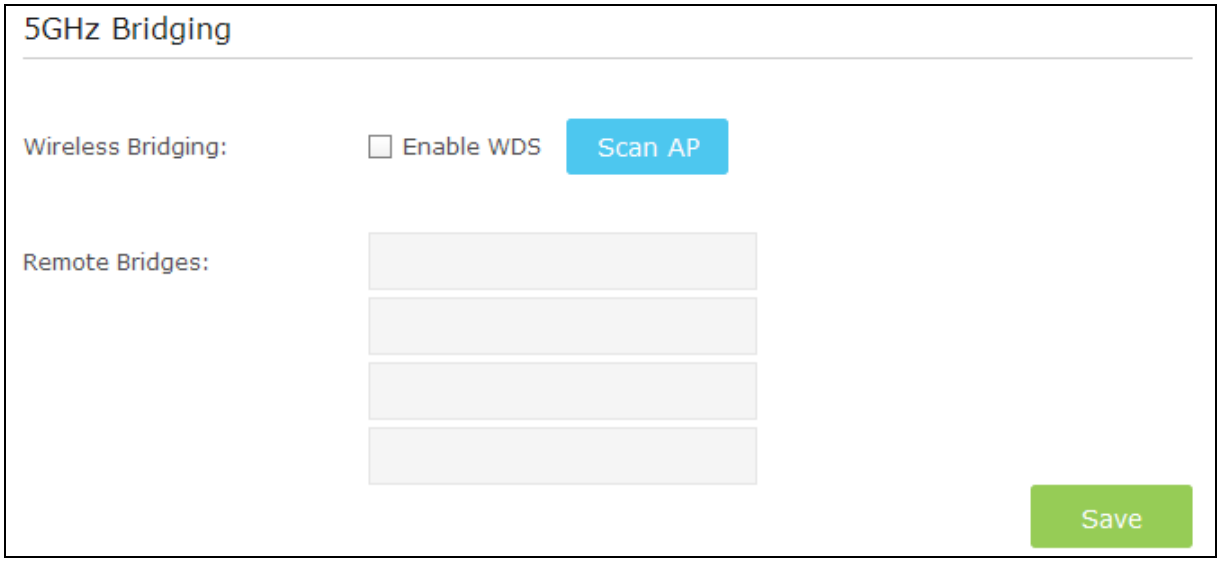


Figure 5-34

- **WDS Bridging -** With this function, the modem router can bridge more WLANs. If you check the **Enable WDS**, you can click the **Scan AP** button to scan the nearby wireless access points.
- **Remote Bridges –** Enter the MAC address the AP your modem router is going to connect to as a client. You can also use the Scan AP function to select the BSSID to join.

Click the **Save** button to save the settings.

5.5.6 Wireless Advanced

Choose menu "**Advanced → Wireless 5G → Wireless Advanced**", you can configure the advanced settings of your wireless network.

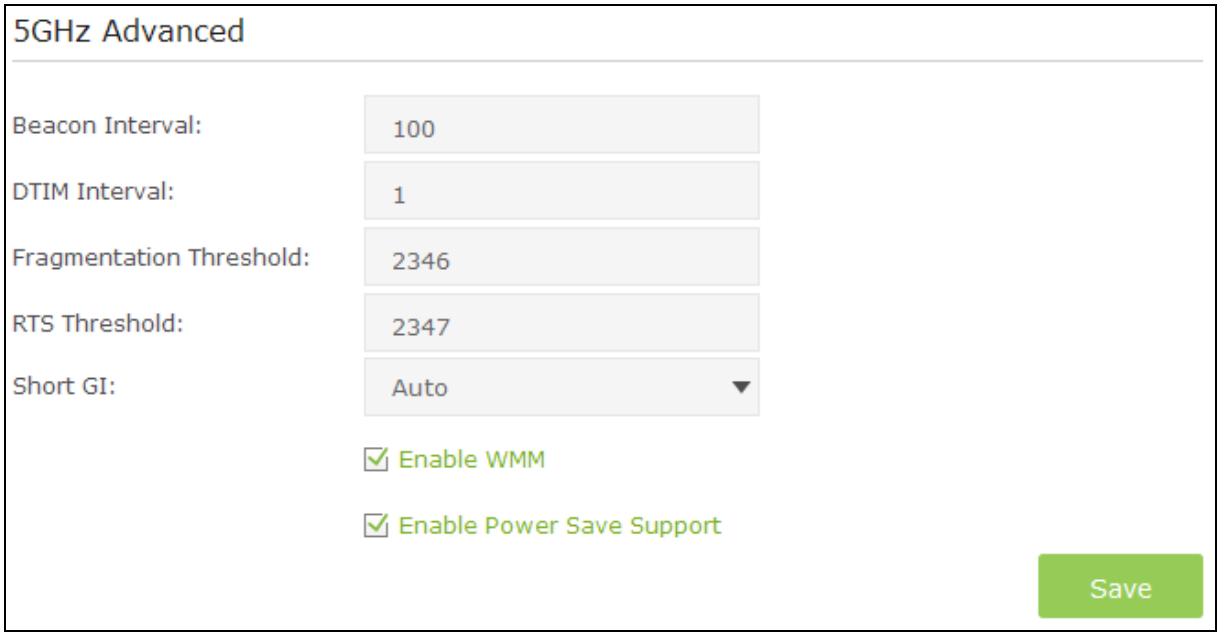


Figure 5-35

5GHz Advanced:

- **Beacon Interval -** Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the modem router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the modem router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the modem router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.

- **Short GI Feature -** This function is recommended for it will increase the data capacity by reducing the guard interval time. Short GI is enabled by default.
- **Enable WMM –** Check the box to enable this function. WMM function can guarantee the packets with high-priority messages being transmitted preferentially, which is strongly recommended. It is enabled by default.
- **Enable Power Save Support -** Check the box to enable this function. This function can make the wireless client has only antenna is in working condition, and the remaining antennas are dormant, so as to achieve the purpose of saving power.

Click the **Save** button to save the settings.

5.6 NAT Forwarding

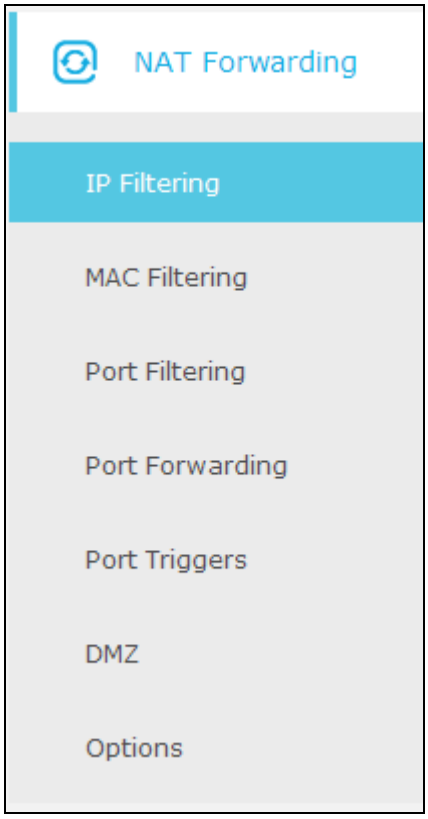


Figure 5-36 The Forwarding menu

There are seven submenus under the Forwarding menu: **IP Filtering**, **MAC Filtering**, **Port Filtering**, **Port Triggers, DMZ** and **Options**. Click any of them, and you will be able to configure the corresponding function.

5.6.1 IP Filtering

Choose menu "**Advanced → NAT Forwarding → IP Filtering**", and then you can control the client's access by configuring the **IP Filtering** function.

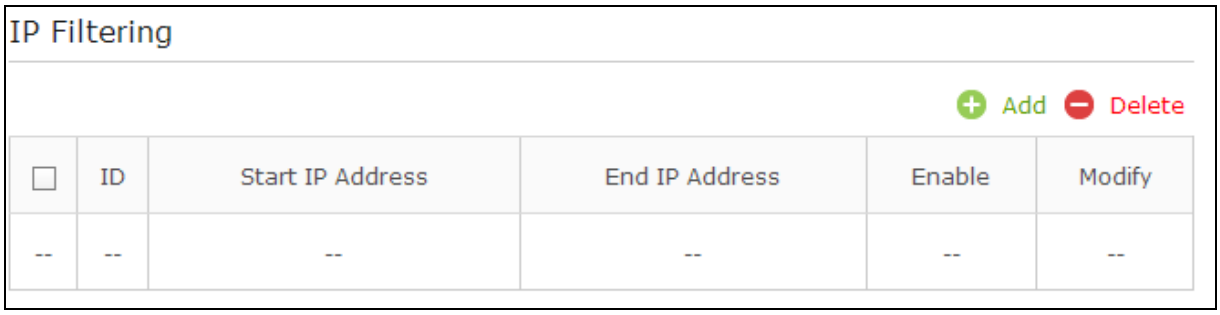


Figure 5-37

To add a IP Address Filtering entry:

1. Click Add button, then you will see a setting page.
2. Enter the **Start IP Address** and the **End IP Address.**
3. Check **Enable this Entry** for this entry, as shown in the following figure.

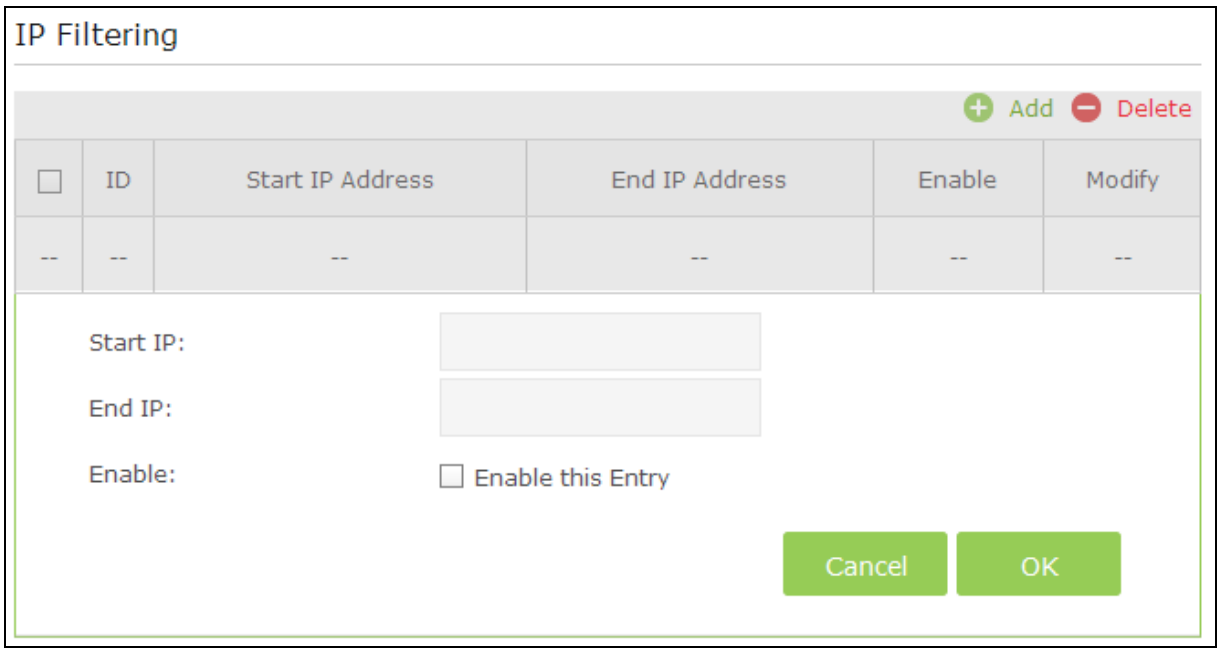


Figure 5-38

4. Click the **OK** button to save this entry. If you do not want to save this entry, click the **Cancel** button.

5.6.2 MAC Filtering

Choose menu "**Advanced → NAT Forwarding → MAC Filtering**", and then then you can control the client's access by configuring the **MAC Filtering** function.

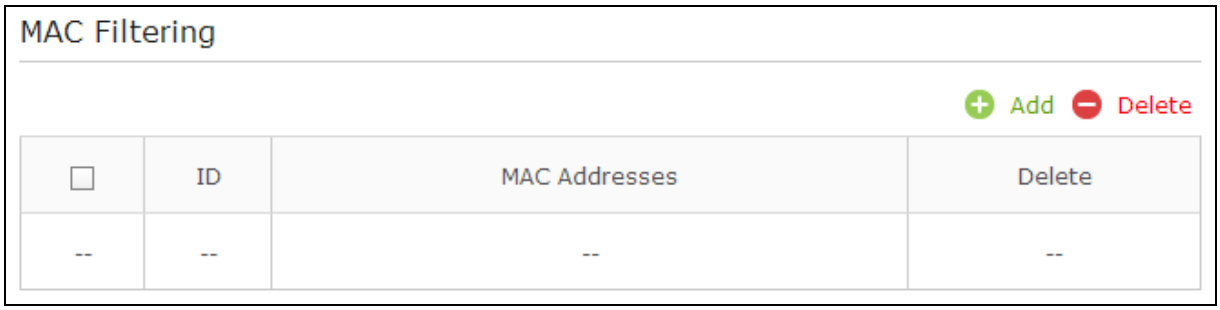


Figure 5-39

To add a MAC Address Filtering entry:

1. Click Add button, then you will see a setting page.
2. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.

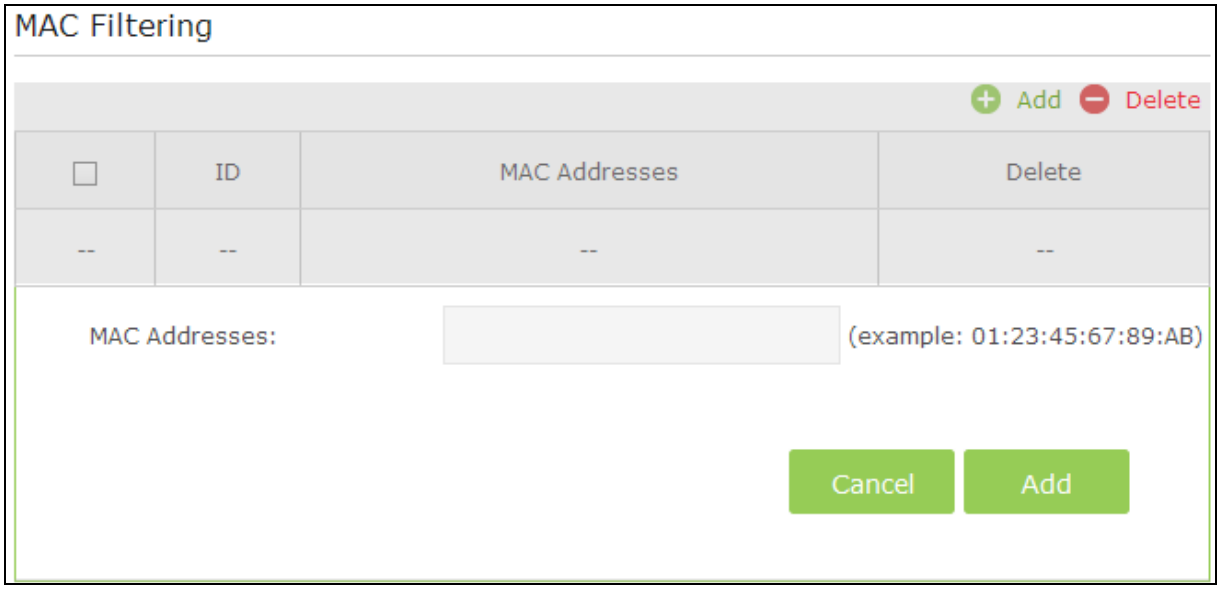


Figure 5-40

3. Click the **Add** button to save this entry. If you do not want to save this entry, click the **Cancel** button.

5.6.3 Port Filtering

Choose menu "**Advanced → NAT Forwarding → Port Filtering**", and then then you can control the client's access by configuring the **Port Filtering** function.

Figure 5-41

To add a IP Address Filtering entry:

1. Click Add button, then you will see a setting page.
2. Enter the **Start Port** and the **End Port.**
3. Select the **Protocol** which you want.
4. Check **Enable this Entry** for this entry, as shown in the following figure.

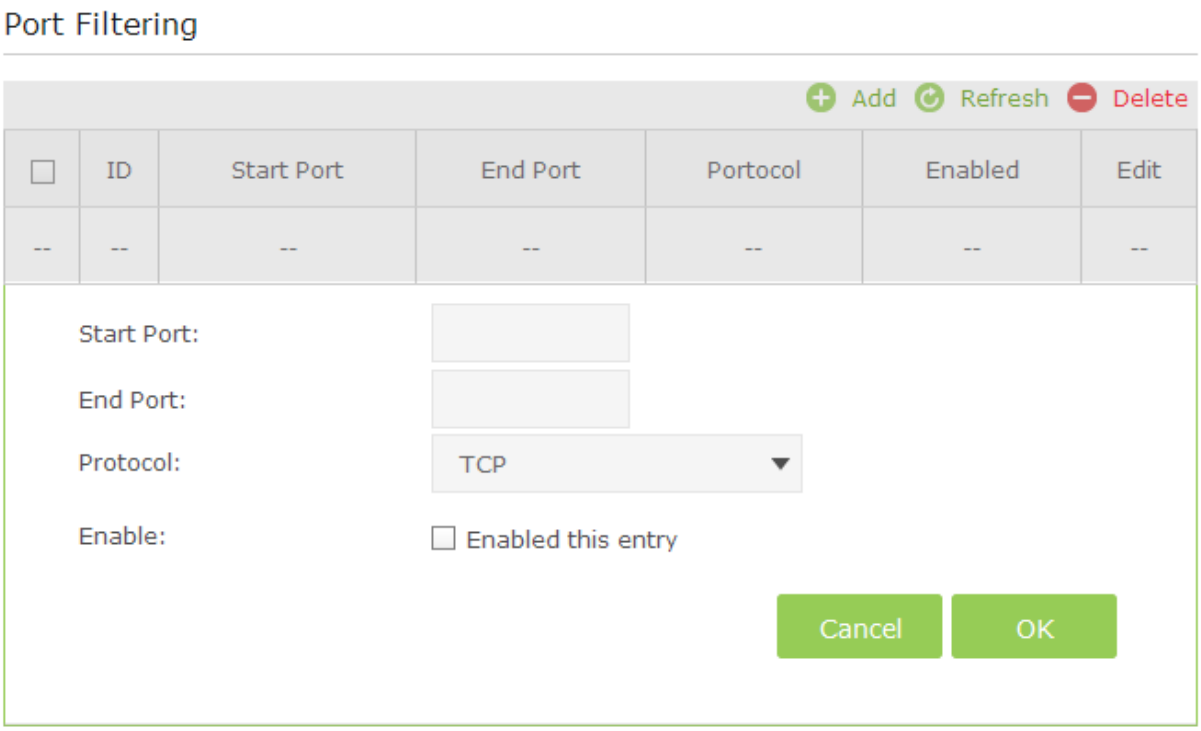
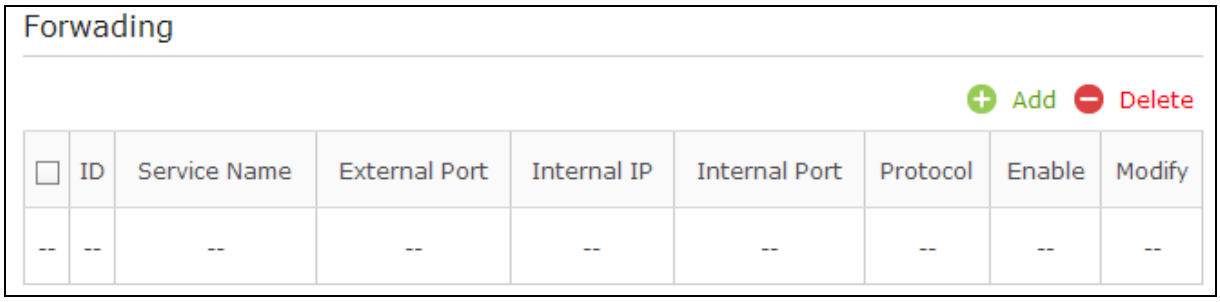


Figure 5-42

5. Click the **OK** button to save this entry. If you do not want to save this entry, click the **Cancel** button.

5.6.4 Port Forwarding

Choose menu "**Advanced → NAT Forwarding → Port Forwarding**", and then then you will see the screen as shown below.



- **Service Name** - The virtual server you want to use.

- **External Port** - The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX – YYY; XXX is the Start port and YYY is the End port).
- **Internal IP** - The IP address of the PC running the service application.
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **External Port** is a single one.
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Enable –** Click the icon to enable the function. If this function has taken effect, the icon will become .
- **Modify –** Click the icon to edit the corresponding entry. If you want to delete this entry, you can click the icon.

To setup a virtual server entry:

1. Click the **Add** button.
2. Enter the **Service Name**.
3. Enter the external port of the computer running the service application in the **External Port** field.
4. Enter the IP address of the computer running the service application in the **Internal IP** field.
5. Enter the internal port of the computer running the service application in the **Internal Port** field.
6. Select the protocol used for this application in the **Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
7. Enable the **Enabled this entry** checkbox.
8. Click the **OK** button.

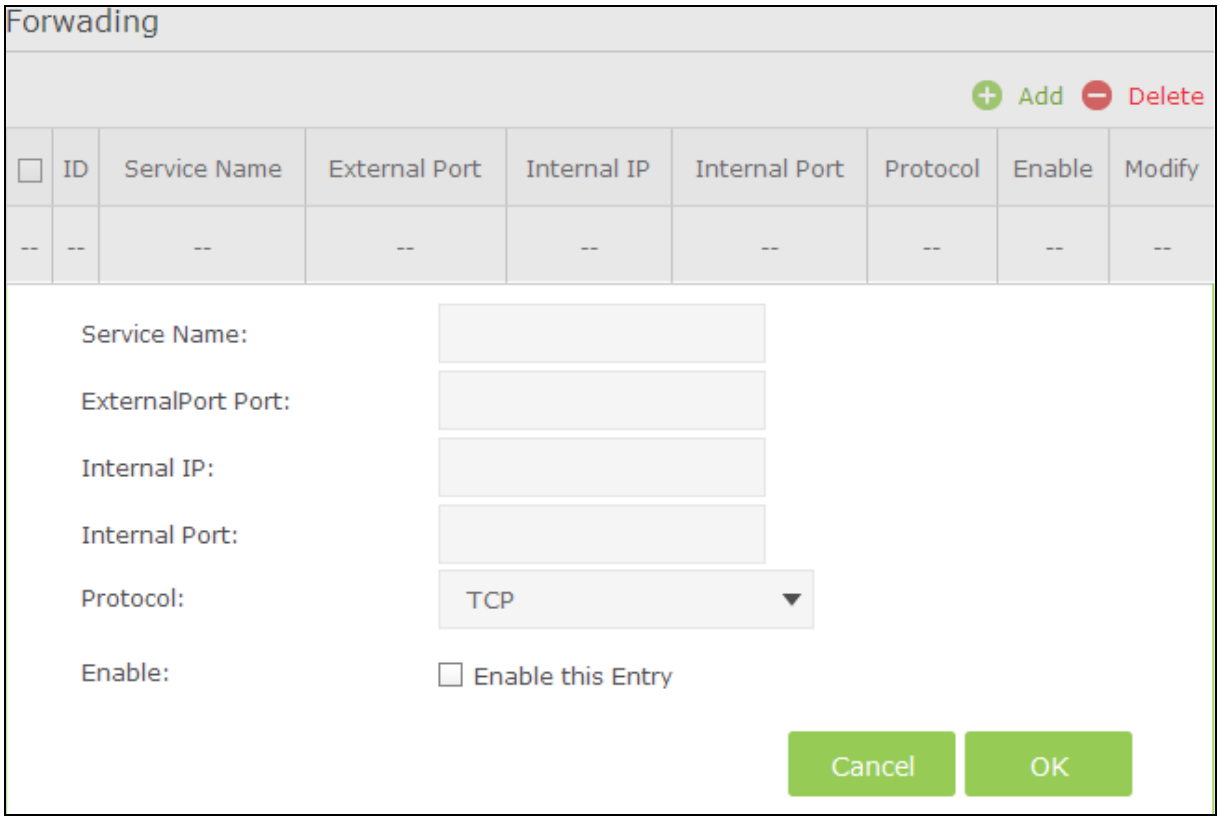


Figure 5-43

Note:

1. It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and type the same IP address for that computer or server.
2. If you set the service port of the virtual server as 80, you must set the Web management port on **Advanced→Security→Remote Management** page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

5.6.5 Port Triggers

Choose menu "**Advanced→ NAT Forwarding→Port Triggering**", you can view and add port triggering in the next screen shown in Figure 5-42. Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. Port Triggering is used for some of these applications that cannot work with a pure NAT modem router.

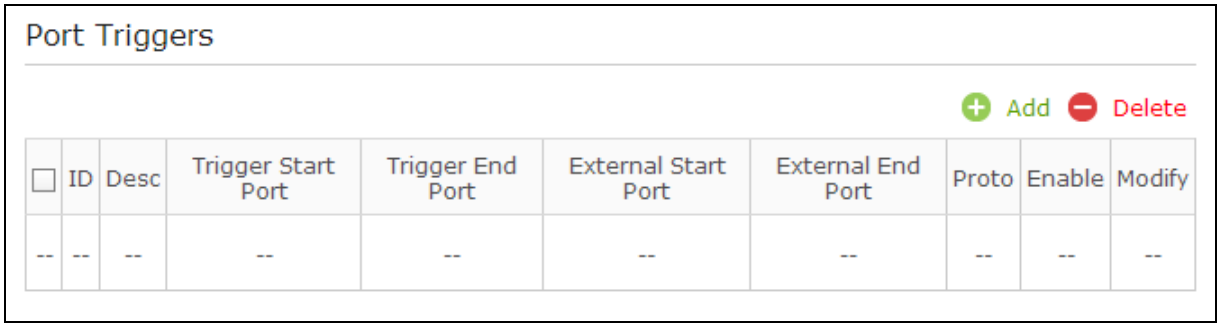


Figure 5-44 Port Triggering

- **Applications** - The applications you want to use.
- **Triggering Port** - The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Triggering Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **External Port** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",", for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **External Protocol** - The protocol used for **External Port**, either **TCP**, **UDP**, or **ALL** (all protocols supported by the router).
- **Enable –** Click the icon to enable the function. If this function has taken effect, the icon will become .
- **Modify –** Click the icon to edit the corresponding entry. If you want to delete this entry, you can click the icon.

To add a new rule, follow the steps below.

1. Click the **Add** button.
2. Select an available interface from the **Interface Name** drop-down list.
3. Click the **View Service** button to select the application you want to use. Then the number of the **Triggering port** and **External Port** will be auto-configured according to your selection. If the **View Service** menu does not list the application that you want to use, enter the **Application**, the number of the **Triggering port** and **External Port**.
4. Select the protocol used for this application in the **Triggering protocol** and **External Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
5. Enable the **Enabled this entry** checkbox.
6. Click the **OK** button.

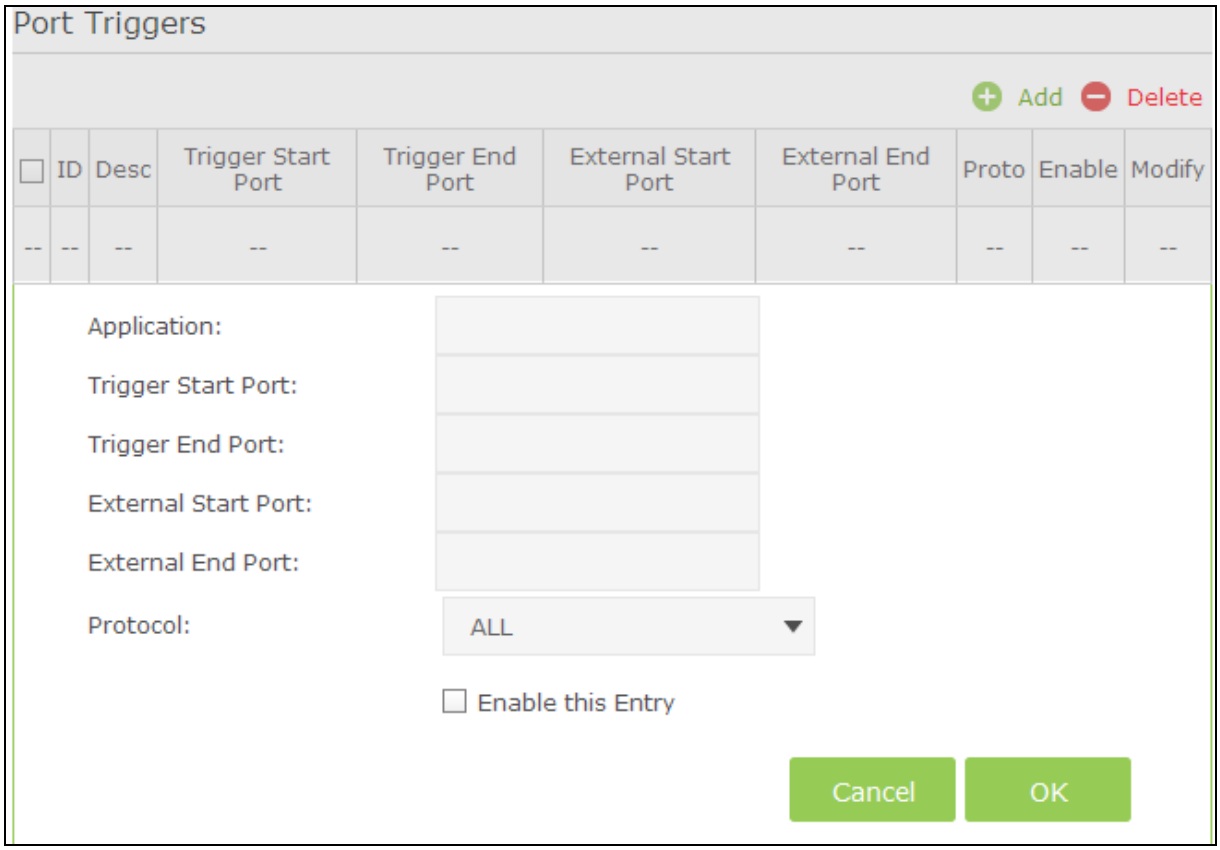


Figure 5-45 Add or Modify a Triggering Entry

Note:

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **External Port** ranges cannot overlap each other.

5.6.6 DMZ

Choose menu "**Advanced → NAT Forwarding → DMZ**", and then you can view and configure DMZ host in the screen shown in Figure 5-44. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. The router forwards packets of all services to the DMZ host. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

Figure 5-46 DMZ

To assign a computer or server to be a DMZ server:

1. Select the **Enable DMZ** checkbox.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Apply** button.

5.6.7 Options

Choose menu "**Advanced → NAT Forwarding → Options**", and then you can view the information in the screen shown in Figure 5-45.

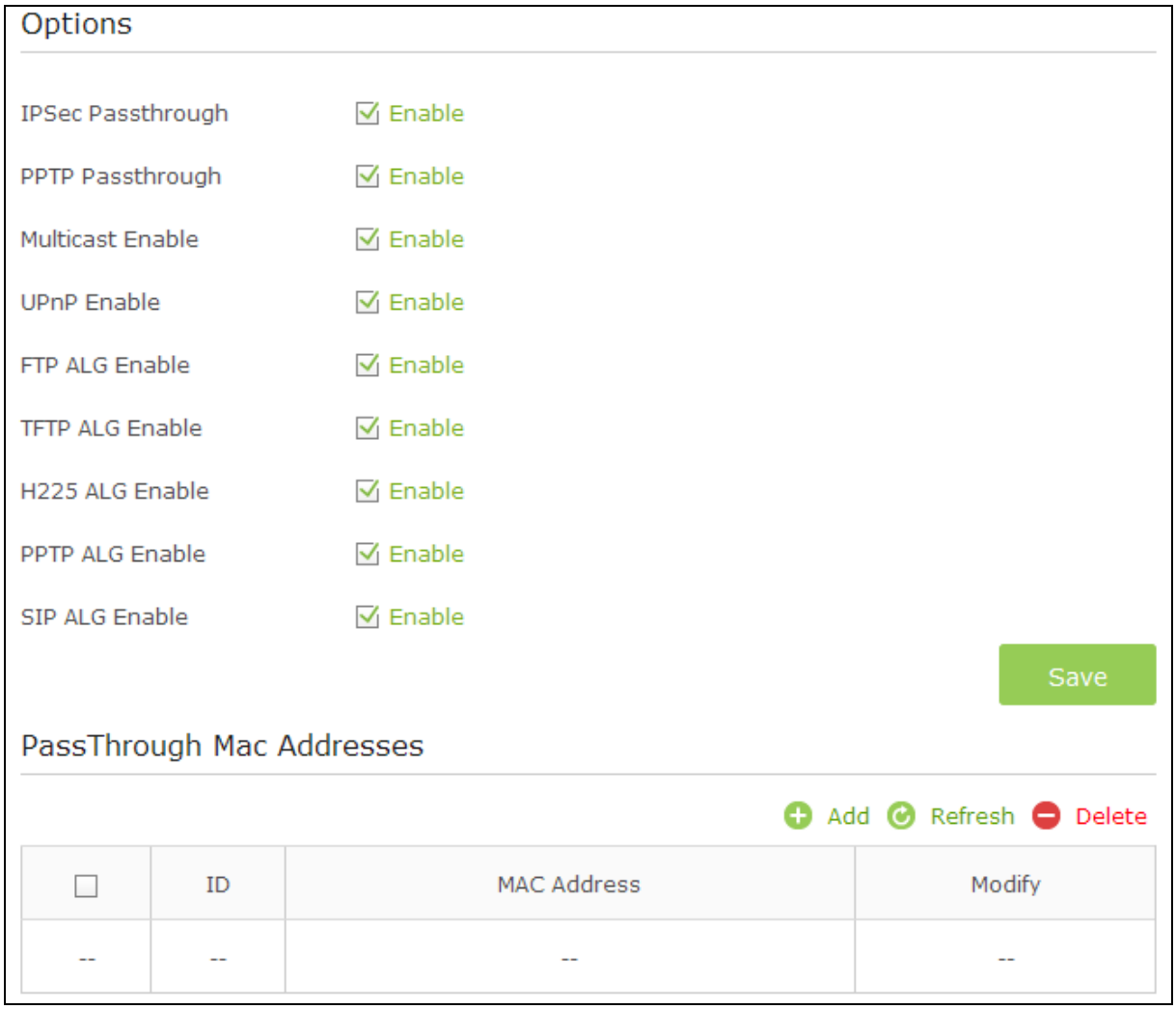


Figure 5-47

5.7 USB Settings

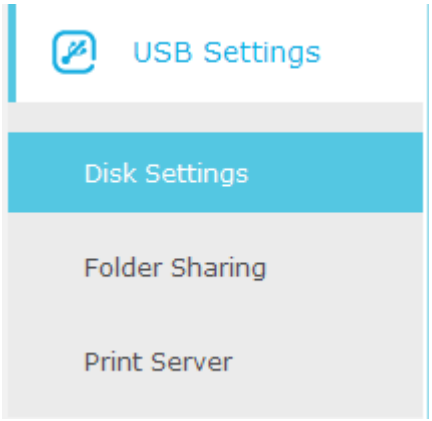


Figure 5-48 The USB Settings menu

There are four submenus under the USB Settings menu (shown in Figure 5-46): **Disk Settings**, **Folder Sharing** and **Print Server**. Click any of them, and you will be able to configure the corresponding functions.

5.7.1 Disk Settings

Choose menu "**Advanced→USB Settings→Disk Settings**", you can configure the USB disk drive attached to the modem router and view the information.

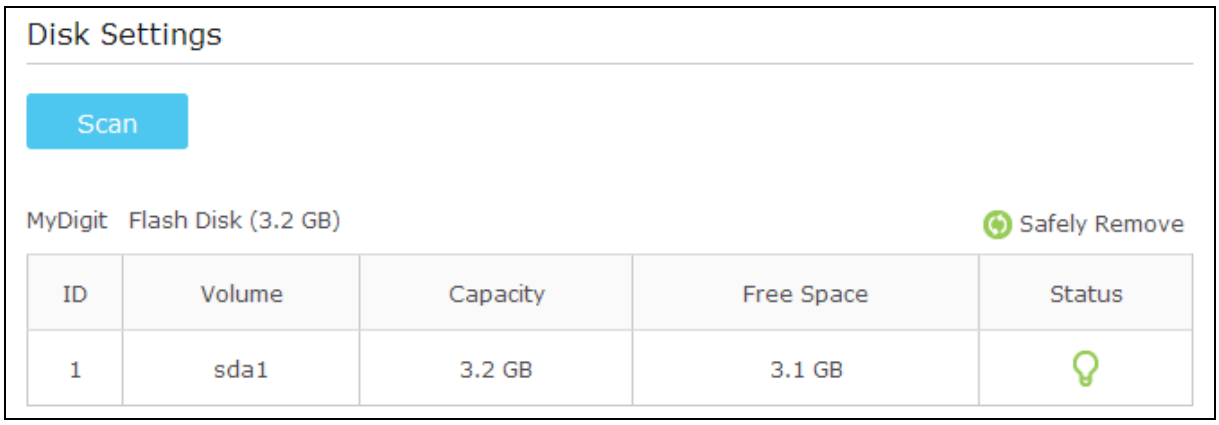


Figure 5-49 Device Settings

Click the **Scan** button to scan the USB drive connected to the router.

- **Volume** - The volume name of the USB drive the users have access to.
- **Capacity** - The storage capacity of the USB driver.
- **Free Space**- The available space of the USB driver.
- **Status:** When the volume is shared, you can click the icon to stop sharing the volume; when volume is non-shared, you can click to icon share the volume.

Click **Safely Remove** button to remove the USB storage device that is connected to USB port.

5.7.2 Folder Sharing

Choose menu "**Advanced→USB Settings→Folder Sharing**", you can configure the sharing account and sharing settings.

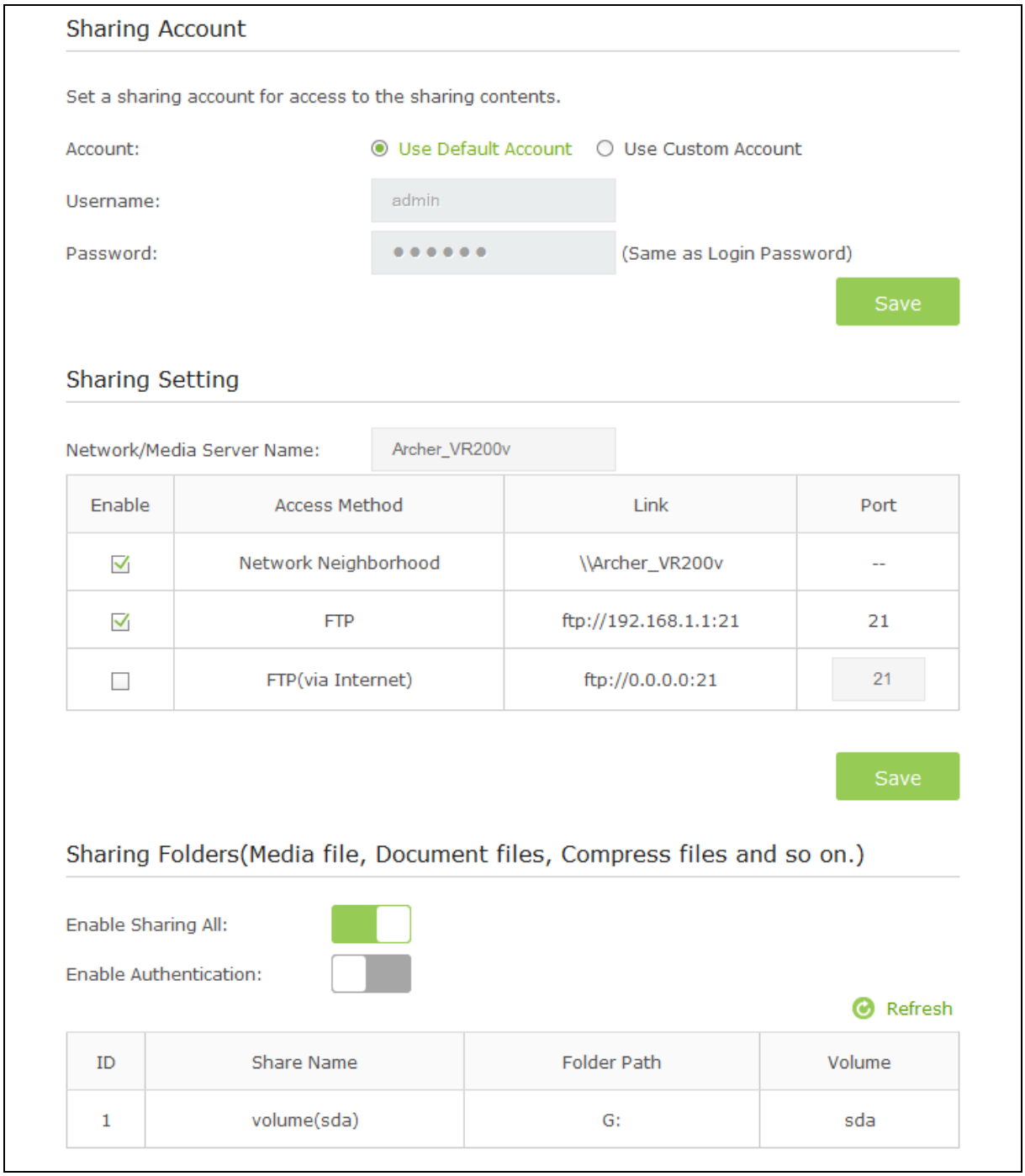


Figure 5-50 Folder Sharing

Sharing Account

- Account – You can select **Use Default Account** or **Use Custom Account** to log in sharing Folders.

  - **Use Default Account -** Select this radio button, and the sharing account username is **admin**, and password is the same as Login Password.

  - **Use Custom Account -** Select this radio button, then you have to specify the new username and password in the **Username** and **Password** fields for sharing account.

Click **Save** button to save these settings.

Sharing Settings

- **Network/Media Server Name -** Show the name of the network/media server. This is the name used to access the USB device connected to the router.
- **Access Method -** Select the check boxes for the access methods that you want.

  1) **Network Neighborhood:** This method is enabled by default. To access the USB drive for example from a Windows computer:

     i. Select **Start > Run**.

     ii. Enter \\LAN IP in the dialog box and click the **OK** button. The default address is \\192.168.1.1.

  2) **FTP:** This method is enabled by default. If you select this check box and click the **Save** button, the LAN users can access the USB drive through FTP. To access the USB drive for example from a Windows computer:

     i. Select **Start > Run**.

     iii. Enter ftp://LAN IP:port in the dialog box and click the **OK** button. The default address is ftp://192.168.1.1:21.

  3) **FTP (via Internet):** This method is disabled by default. If you select this check box, remote users can access the USB drive through FTP over the Internet. This feature supports both downloading and uploading of files. To access the USB drive for example from a Windows computer:

     i. Select **Start > Run**.

     ii. Enter ftp://WAN IP:port in the dialog box and click the **OK** button.

☞ **Note:**

1. If the LAN IPv4 is changed, the link for access Network Neighborhood and FTP will be changed to the same IP address.
2. If the port for FTP (via Internet) is changed, the port for FTP will be changed to the same port.

Sharing Folders (Media file, Document files, Compress files and so on.)

- **Enable Sharing All -** The switch for sharing all the folders. If you turn on the switch, the field will become green and all the folders in the USB drive will be shared.
- **Enable Authentication -** If you turn on this switch, the folder sharing needs authentication. The default setting is off.

To share the folders you specified, please follow the steps below.

1. Turn off the **Enable Sharing All** switch and the next screen will pop-up as shown in Figure 5-49.

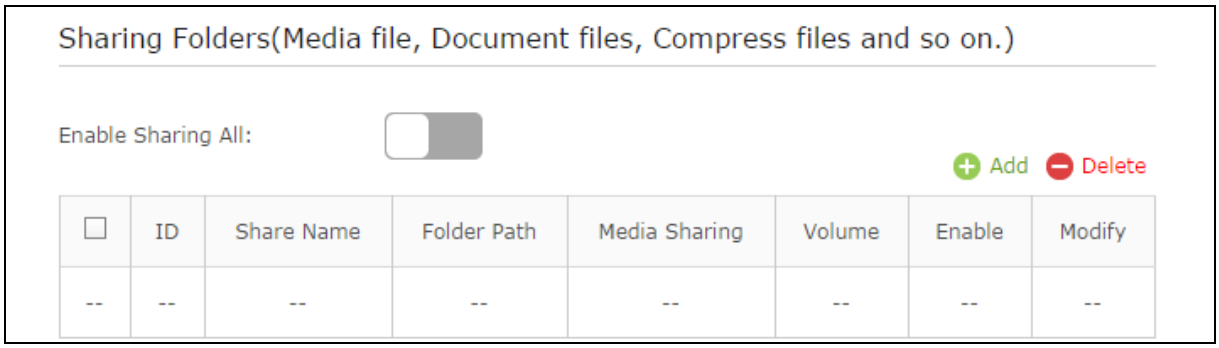


Figure 5-51 Add or Modify Share Folder

2. Click the **Add** button and the next screen will pop-up as shown in Figure 5-50.

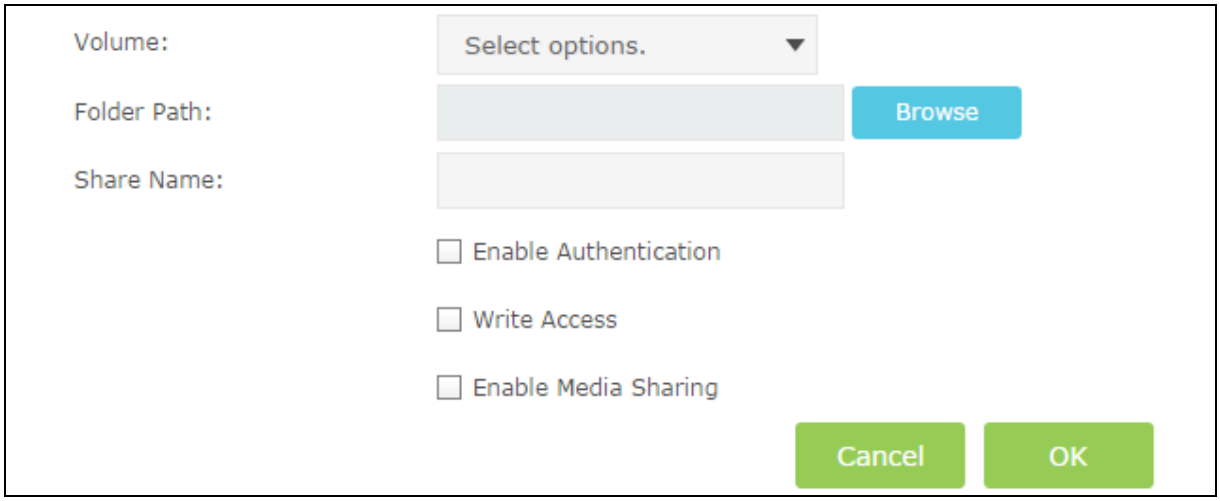
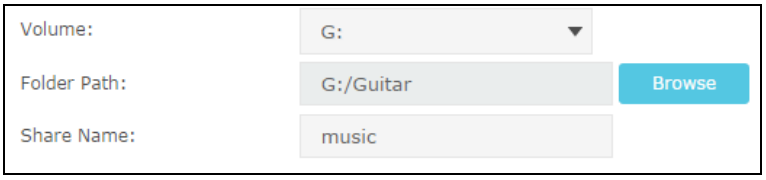


Figure 5-52 Add Share Folder

3. Select the volume desired to share from the **Volume** drop-down list. Then click the **Browse** button to select the folder path. You can create a share name, e.g. image.



4. Select the checkboxes in Figure 5-50.according to your needs.

- **Enable Authentication -** If this checkbox is selected, then the folder sharing needs authentication.
- **Write Access -** If this checkbox is selected, then the sharing folder is allowed write access.
- **Enable Media Sharing -** Select this checkbox to enable media sharing.

5. Click **OK** to complete the settings.

5.7.3 Print Server

Please refer to Section 4.6.2 Print Server.

5.8 Firewall

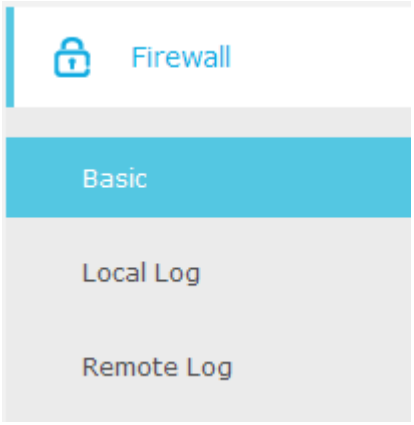


Figure 5-53 The Firewall menu

There are three submenus under the Security menu: **Basic, Local Log**, and **Remote Log**. Click any of them, and you will be able to configure the corresponding functions.

5.8.1 Basic

Choose menu "**Advanced → Firewall → Basic**", and you can configure the basic firewall function.

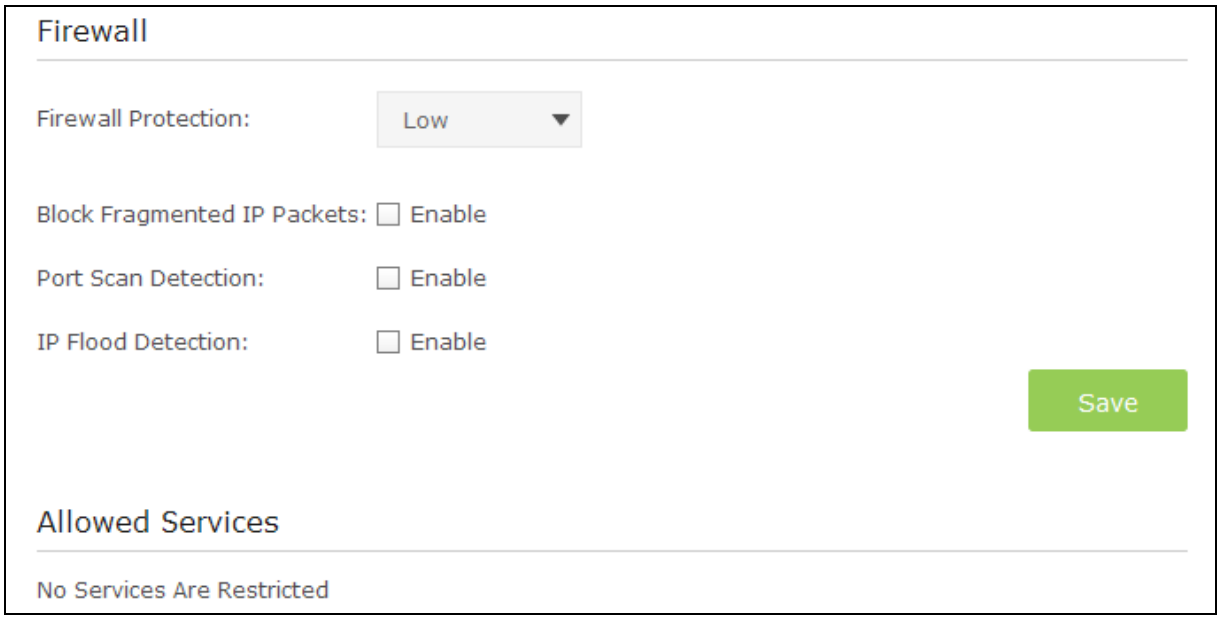


Figure 5-54

Firewall:

- **Firewall Protection -** You can select **Off, Low**, **Medium** or **High** which you would like.

Click the **Save** button to save your settings.

5.8.2 Local Log

Choose menu "**Advanced→ Firewall → Local Log**", and then you can configure the function in the screen as shown in Figure 5-53.

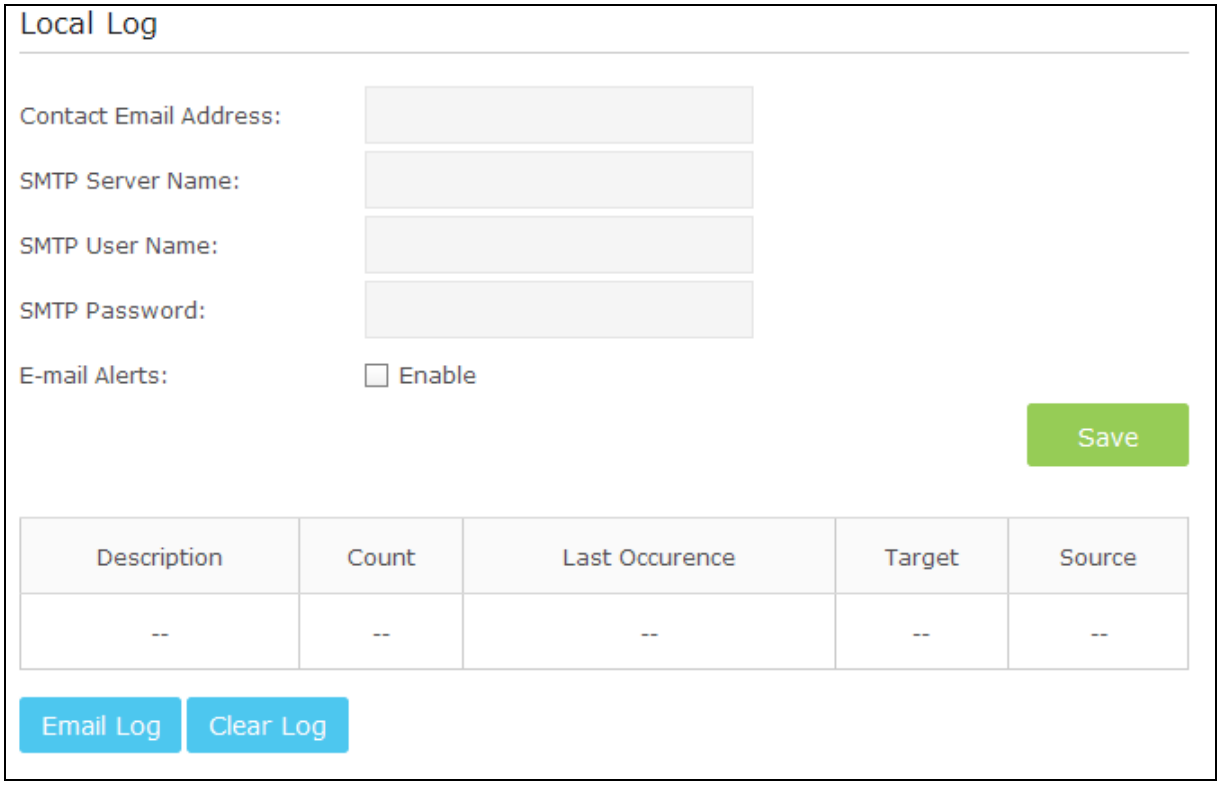


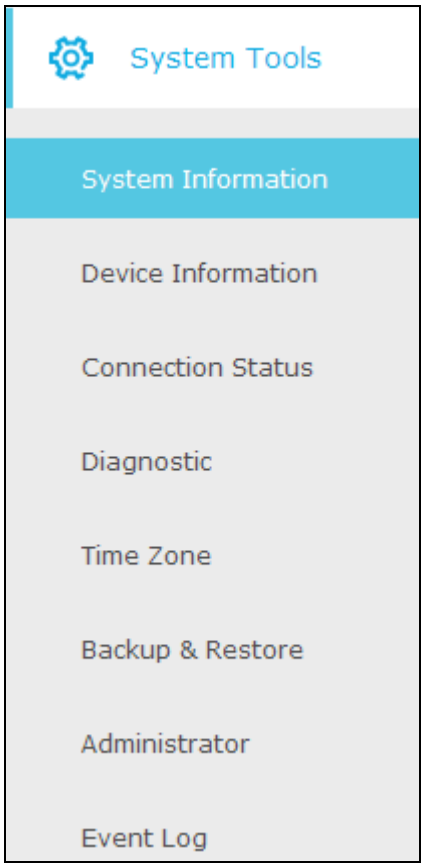
Figure 5-55

5.8.3 Remote Log

Choose menu "**Advanced→ Firewall → Remote Log**", and then you can configure the function in the screen as shown in Figure 5-532.

Figure 5-56

5.9 System Tools



Choose menu "**Advanced→System Tools**", you will see eight submenus under the System Tools menu: **System Information**, **Device Information**, **Connection Status**, **Diagnostic**, **Time Zone**, **Backup & Restore**, **Administrator** and **Event Log.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.9.1 System Information

Choose menu "**Advanced→System Tools→Diagnostic**", you can see the current status information about the modem router.

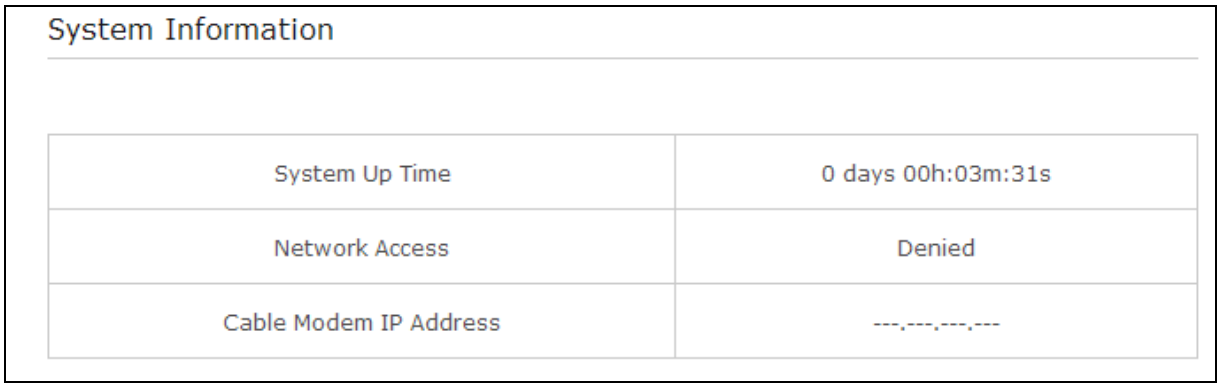


Figure 5-57

5.9.2 Device Information

Choose menu "**Advanced→System Tools→Device Information**", you can see the current information about the modem router.

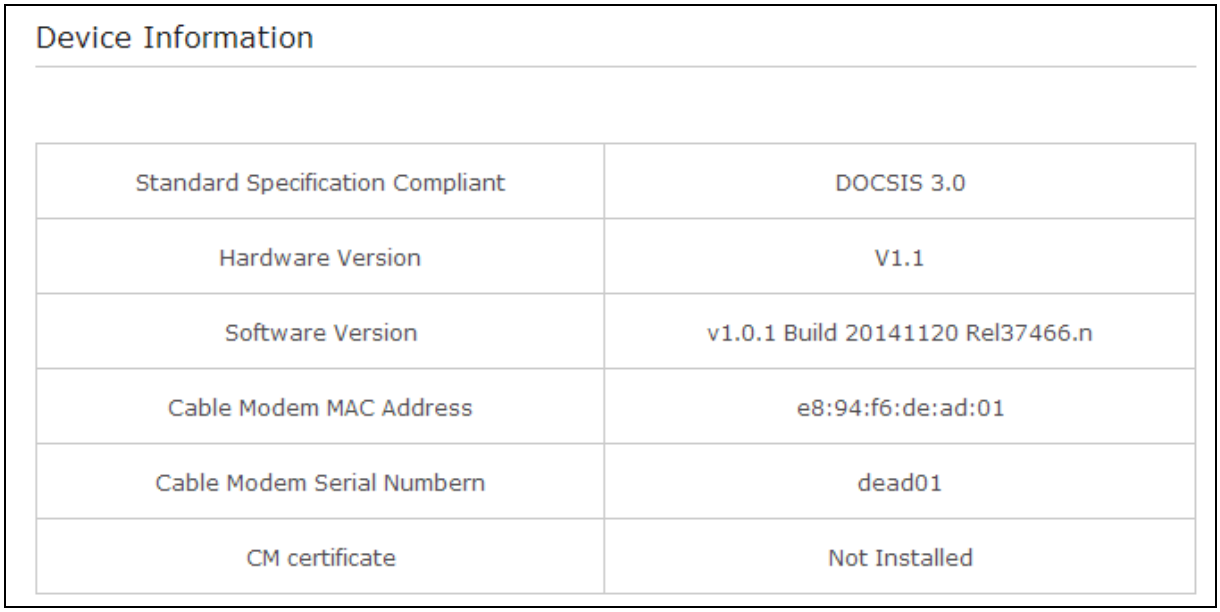


Figure 5-58

5.9.3 Connection Status

Choose menu "**Advanced→System Tools→Device Information**", you can see the current connection status about the modem router.

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	753000000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Configuration File	In Progress	In Progress
Security	Disabled	Disabled

Downstream Bonded Channels

Channel	Status	Modulation	Channel ID	Frequency	Power	SNR
1	Not Locked	unknown	0	729000000 Hz	-16.9 dBmV	0.0 dB
2	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
3	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
4	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
5	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
6	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
7	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
8	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
9	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
10	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
11	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
12	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB
13	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB

Figure 5-59

5.9.4 Diagnostic

Choose menu “**Advanced→System Tools→Diagnostic**”, you can test the connectivity of the Internet on the following screen.

Figure 5-60

Click **Start Test** to check the connectivity of the Internet. The page will display the result of diagnosis.

Note:

Only one user can use the diagnostic tools at one time.

5.9.5 Time Zone

Choose menu "**Advanced→System Tools→Time Settings**", you can configure the time settings on the following screen.

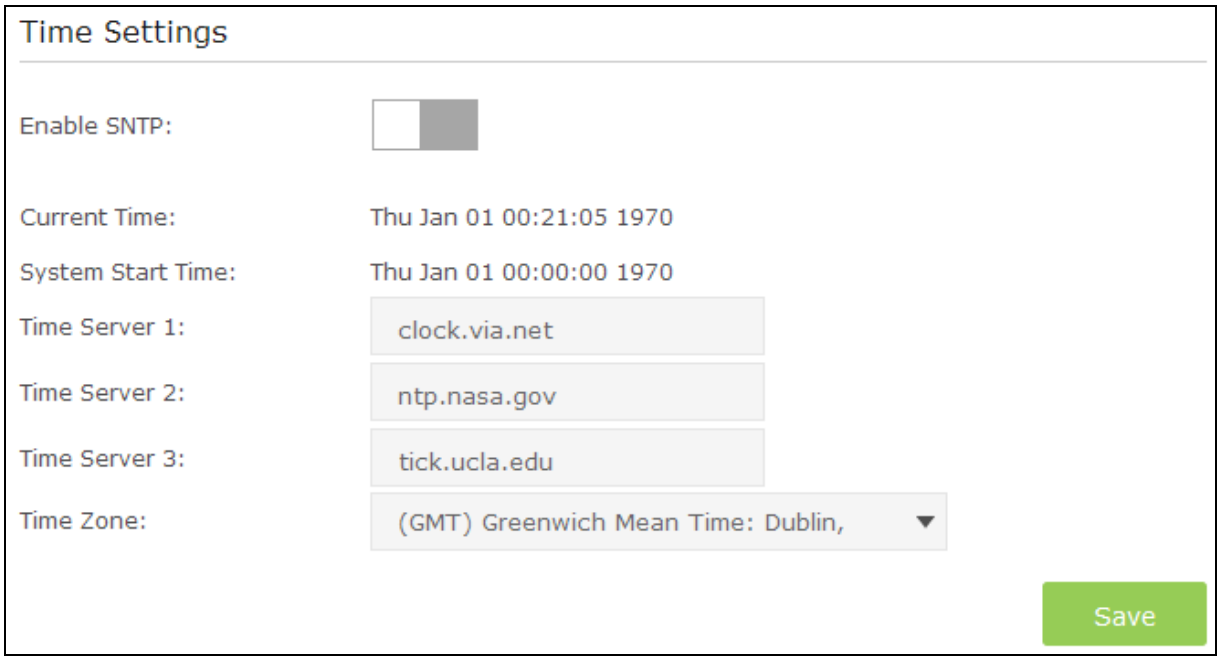


Figure 5-61

Time Settings:

- **Time Zone -** Select your local time zone from the pull down list.
- **Time Server 1 / Time Server 2 / Time Server 3-** Enter the address or domain of the **Server 1** or **Server 2**, and then the modem router will get the time from the Server preferentially. In addition, the modem router built-in some common Servers, so it can get time automatically once it connects the Internet.

Note:

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully; otherwise, these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The router will automatically obtain GMT from the Internet if it is configured accordingly.
4. The Daylight Saving will take effect one minute after the configurations are completed.

5.9.6 Backup & Restore

Choose menu "**Advanced→System Tools→Backup & Restore**", and then you can save the current configuration of the modem router as a backup file and restore the configuration via a backup file as shown in the following figure.

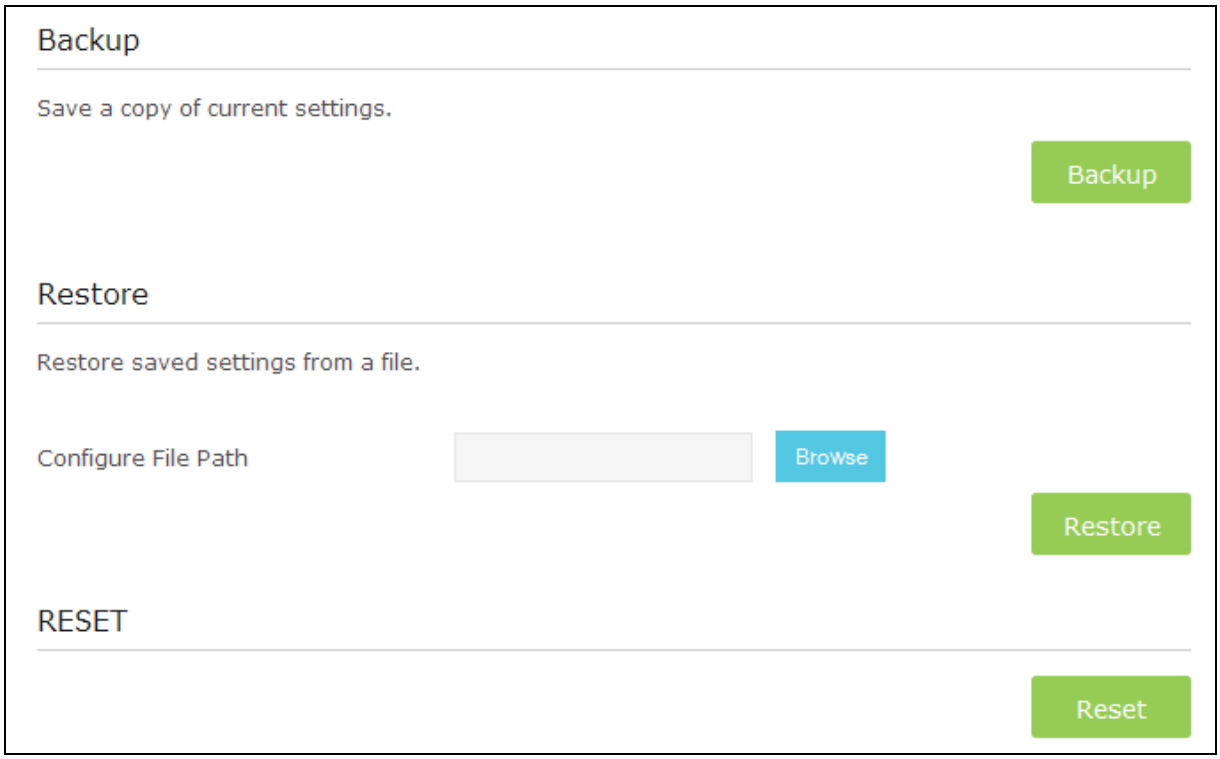


Figure 5-62

Backup:

Click the **Backup** button to save all configuration settings as a backup file in your local computer.

Restore:

To restore the modem router's configuration, follow these instructions.

- Click the **Browse** button to find the configuration file which you want to restore.
- Click the **Restore** button to restore the configuration with the file whose path is the one you have input or selected in the blank.

Reset:

Click the **Reset** button to reset all configuration settings to their default values.

Note:

1. The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the modem router will restart automatically then. Keep the power of the modem router on during the process, in case of any damage.
2. All changed settings will be lost when defaults are restored.

5.9.7 Administrator

Choose menu "**Advanced→System Tools→Administration**", you will see the following screen.

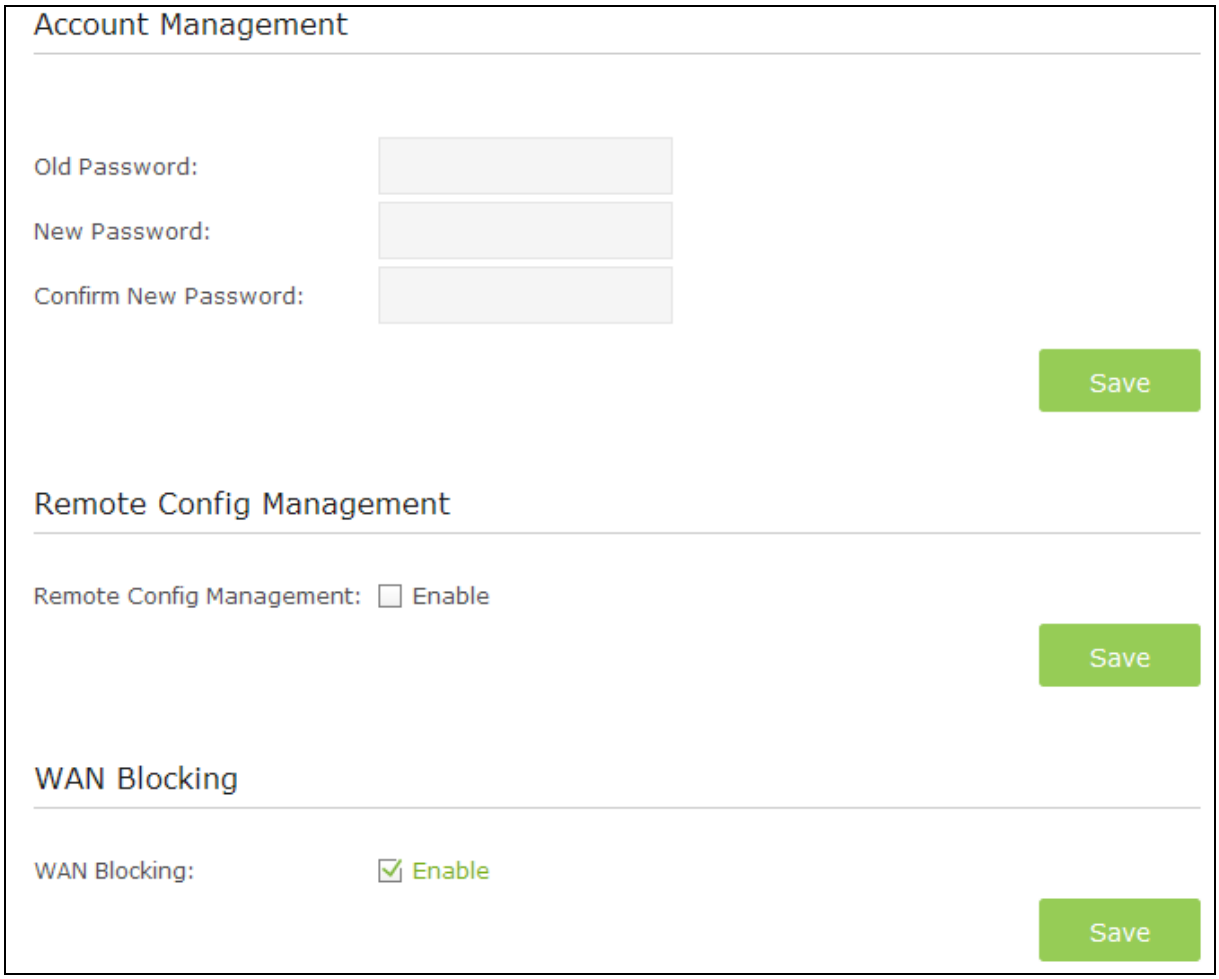


Figure 5-63

Account Management:

Here you can set the account user information about **Old Password**, **New Password and Confirm Password**.

It is strongly recommended that you should change the factory default user name and password of the router, because all users who try to access the router's Web-based utility or Quick Setup will be prompted for the router's default user name and password.

Note:

Enter the new Password twice to confirm it. The level of the new password's security will be shown on the screen as **Low**, **Middle** or **High**.

Click the **Save** button save the settings.

Remote Management:

- **Remote Management –** Check the **Enable** to enable the remote management.

  Note:

  To access the router, you should type your router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for

the router's password. After successfully entering the username and password, you will be able to access the router's web-based utility.

5.9.8 Event Log

Choose menu "**Advanced→System Tools→Event Log**", and then you can view and clear the logs of the modem router.

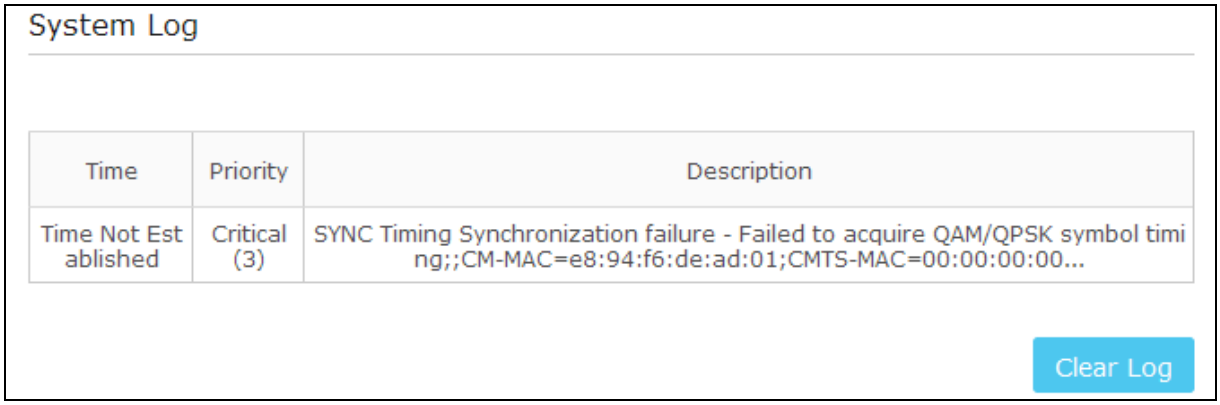


Figure 5-64

Appendix A: Specifications

HARDWARE FEATURES	
Interface	1 F-Connector, female 75 Ω 4 10/100/1000Mbps RJ45 LAN Ports 2 USB 2.0 Ports
Button	1 Power On/Off Button 1 Wi-Fi On/Off Button 1 WPS Button 1 Reset Button
External Power Supply	12VDC/3.5A
IEEE Standards	IEEE 802.3, 802.3u
DOCSIS Standards	DOCSIS 3.0 DOCSIS 2.0 DOCSIS 1.1 DOCSIS 1.0
Dimensions (W x D x H)	2.5× 7.7× 9.7 in. (62.5× 195× 246 mm)
Antenna Type	Omni directional, Internal
Antenna Gain	3×5 dBi for 2.4GHz and 5GHz
DOCSIS Downstream	
Channel Binding	Up to 16
Modulation	64 /256 / 1024 QAM
Maximum PHY Rate	DOCSIS Up to 680 Mbps
Bandwidth	DOCSIS 96 MHz(16 channels) / 6MHz (single channel)
Frequency Range	108 to 1002 MHz (edge to edge)

HARDWARE FEATURES		
Frequency Plan	DOCSIS Annex B	
Symbol Rate	DOCSIS 64 QAM 5.057 Msym/s; 256 QAM 5.361 Msym/s	
Operating Level Range	-15 to 15 dBmV (DOCSIS)	
Security	DOCSIS 3.0 Security (BPI+, EAE, SSD)	
DOCSIS UPSTREAM		
Channel Binding	Up to 4	
Modulation	QPSK and 8, 16, 32, 64, 128, 256 QAM	
Maximum PHY Rate	Up to 30Mbps for Single Channel and 4p to 120 Mbps for 4 channel bonding both for DOCSIS	
Channel Bandwidth	200 kHz, 400 kHz, 800 kHz, 1.6 MHz,3.2 MHz, 6.4 MHz	
Frequency Range	DOCSIS 5-42 MHz (edge to edge),	
Symbol Rate	160, 320, 640, 1280, 2560, 5120 ksym/s	
Level range	TDMA	Pmin to +57 dBmV (32 QAM, 64 QAM) Pmin to +58 dBmV (8 QAM, 16 QAM) Pmin to +61 dBmV (QPSK)
	Note: TDMA max output power reduced 3dB when transmitting two channels and 6dB when transmitting 3 or 4 channels	
	S-CDMA	Pmin to +56 dBmV (all modulations) Pmin = +17 dBmV, 1280 kHz modulation rate Pmin = +20 dBmV, 2560 kHz modulation rate Pmin = +23 dBmV, 5120 kHz modulation rate
	Note: S-CDMA max output reduced 3dB when transmitting 2 or more channels	
WIRELESS FEATURES		

WIRELESS FEATURES	
Wireless Standards	IEEE 802.11ac/n/a 5GHz IEEE 802.11b/g/n 2.4GHz
Wireless Speeds	5GHz: Up to 1300Mbps 2.4GHz: Up to 450Mbps
Frequency	2.4GHz and 5GHz
EIRP	<20dBm(EIRP)
Wireless Functions	Enable/Disable Wireless Radio, WDS Bridge, WMM, Wireless Statistics
Wireless Security	64/128-bit WEP,WPA / WPA2,WPA-PSK/ WPA2-PSK encryption, Wireless MAC Filtering
Guest Network	2.4GHz guest network × 1 5GHz guest network × 1
Wireless Schedule	Support 2.4GHz and 5GHz Wireless Schedule
WPS	Support PIN and Push button

SOFTWARE FEATURES	
WAN Connection Type	Dynamic IP、Static IP、L2TP（Dynamic）、L2TP（Static）
DHCP	Server, Client, DHCP Client List,
Port Forwarding	Virtual Server, Port Triggering, DMZ, ALGs
USB Sharing	Support Samba(Storage)/FTP Server/Media Server/Printer Server
Dynamic DNS	DynDns, NO-IP
IPv6	IPv6 and IPv4 dual stack
Security	NAT Firewall, SPI Firewall, Access Control, IP and MAC Address Binding, Denial of Service(DoS), SYN Flooding, Ping of Death MAC / IP / Port/ URL Filtering, Baseline Encryption (BPI)/ BPI+/ EAE/ SSD

SOFTWARE FEATURES	
Management	Web Based Configuration(HTTP), Command Line Interface; Remote management, SSL for TR-069, SNMP v1/v2c/v3; Diagnostic Tools
Advanced Features	Parental Control, Network Address Translation (NAT); RIP v1/v2(optional); DNS, DNS Relay, IGMP V1/V2/V3, UPnP

OTHERS	
Certification	FCC, RoHS, CableLabs, UL
Package Contents	Archer CR700 RJ-45 Ethernet Cable Quick Installation Guide Power Adapter
System Requirements	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™, Windows 7, Windows 8, MAC® OS, NetWare®, UNIX® or Linux.
Environment	Operating Temperature: 0℃~40℃ (32℉~104℉) Storage Temperature: -40℃~70℃ (-40℉~158℉) Operating Humidity: 10%~90% non-condensing Storage Humidity: 5%~90% non-condensing

Appendix B: Technical Support

Technical Support

- For more troubleshooting help, go to:
  http://www.tp-link.com/en/support/faq
- To download the latest Firmware, Driver, Utility and User Guide, go to:
  http://www.tp-link.com/en/support/download
- For all other technical support, please contact us by using the following details:

Global

Tel: +86 755 2650 4400

Fee: Depending on rate of different carriers, IDD.

E-mail: support@tp-link.com

Service time: 24hrs, 7 days a week

USA/Canada

Toll Free: +1 866 225 8139

E-mail: support.usa@tp-link.com (USA)
support.ca@tp-link.com (Canada)

Service time: 24hrs, 7 days a week

Turkey

Tel: 0850 7244 488 (Turkish Service)

Fee: Depending on rate of different carriers.

E-mail: support.tr@tp-link.com

Service time: 09:00 to 21:00, 7 days a week

Ukraine

Tel: 0800 505 508

Fee: Free for Landline; Mobile: Depending on rate of different carriers

E-mail: support.ua@tp-link.com

Service time: Monday to Friday, 10:00 to 22:00

Brazil

Toll Free: 0800 608 9799 (Portuguese Service)

E-mail: suporte.br@tp-link.com

Service time: Monday to Friday, 09:00 to 20:00; Saturday, 09:00 to 15:00

Indonesia

Tel: (+62) 021 6386 1936

Fee: Depending on rate of different carriers.

E-mail: support.id@tp-link.com

Service time: Monday to Friday, 09:00 to 18:00,

*Except public holidays

Australia/New Zealand

Tel: NZ 0800 87 5465 (Toll Free)
AU 1300 87 5465 (Depending on 1300 policy.)

E-mail: support.au@tp-link.com (Australia)
support.nz@tp-link.com (New Zealand)

Service time: 24hrs, 7 days a week

Germany/Austria

Tel: +49 1805 875 465 (German Service)
+49 1805 TPLINK
+43 820 820 360

Fee: Landline from Germany: 0.14EUR/min.

Landline from Austria: 0.20EUR/min.

E-mail: support.de@tp-link.com

Service time: Monday to Friday, 09:00 to 12:30 and 13:30 to 18:00. GMT+1 or GMT+2 (DST in Germany) *Except bank holidays in Hesse

Singapore

Tel: +65 6284 0493

Fee: Depending on rate of different carriers.

E-mail: support.sg@tp-link.com

Service time: 24hrs, 7 days a week

UK

Tel: +44 (0) 845 147 0017

Fee: Landline: 1p-10.5p/min, depending on the time of day. Mobile: 15p-40p/min, depending on your mobile network.

E-mail: support.uk@tp-link.com

Service time: 24hrs, 7 days a week

Italy

Tel: +39 023 051 9020

Fee: Depending on rate of different carriers.

E-mail: support.it@tp-link.com

Service time: Monday to Friday, 09:00 to 13:00; 14:00 to 18:00

Malaysia

Toll Free: 1300 88 875 465

Email: support.my@tp-link.com

Service time: 24hrs, 7 days a week

Poland

Tel: +48 (0) 801 080 618

+48 223 606 363 (if calls from mobile phone)

Fee: Depending on rate of different carriers.

E-mail: support.pl@tp-link.com

Service time: Monday to Friday, 09:00 to 17:00. GMT+1 or GMT+2 (DST)

France

Tel: 0820 800 860 (French service)

Fee: 0.118 EUR/min from France

Email: support.fr@tp-link.com

Service time: Monday to Friday, 09:00 to 18:00 *Except French Bank holidays

Switzerland

Tel: +41 (0) 848 800 998 (German Service)

Fee: 4-8 Rp/min, depending on rate of different time.

E-mail: support.ch@tp-link.com

Service time: Monday to Friday, 09:00 to 12:30 and 13:30 to 18:00. GMT+1 or GMT+2 (DST)

Russian Federation

Tel: 8 (499) 754 5560 (Moscow NO.)

8 (800) 250 5560 (Toll-free within RF)

E-mail: support.ru@tp-link.com

Service time: From 09:00 to 21:00 (Moscow time) *Except weekends and holidays in RF